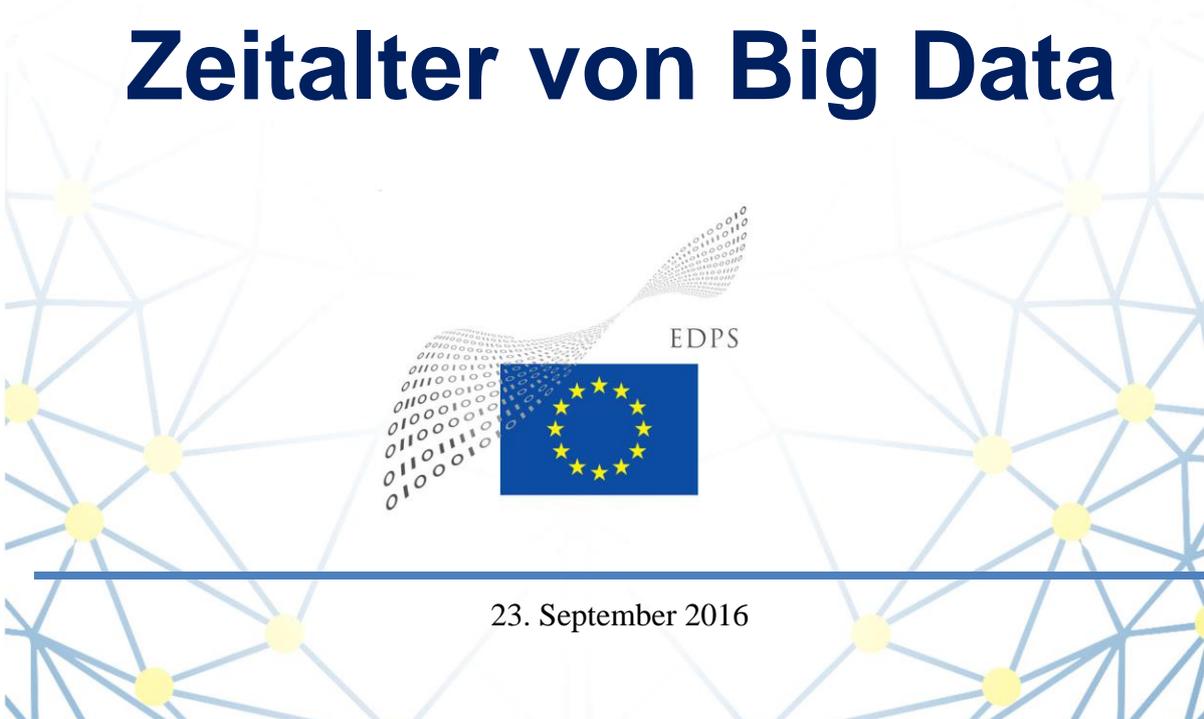


EUROPEAN DATA PROTECTION SUPERVISOR

# Stellungnahme 8/2016

## Stellungnahme des EDSB zur kohärenten Durchsetzung von Grundrechten im Zeitalter von Big Data



23. September 2016

*Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 41 Absatz 2 der Verordnung (EG) Nr. 45/2001 „im Hinblick auf die Verarbeitung personenbezogener Daten ... sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Privatsphäre, von den Organen und Einrichtungen der Gemeinschaft geachtet werden“; er ist „für die Beratung der Organe und Einrichtungen der Gemeinschaft und der betroffenen Personen in allen die Verarbeitung personenbezogener Daten betreffenden Angelegenheiten“ zuständig. Gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 ist die Kommission zur Konsultation des EDSB verpflichtet, „wenn [sie] einen Vorschlag für Rechtsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten annimmt“.*

*Er wurde zusammen mit dem Stellvertretenden Datenschutzbeauftragten im Dezember 2014 ernannt und ausdrücklich mit einem konstruktiven und proaktiven Vorgehen beauftragt. In seiner im März 2015 veröffentlichten Fünf-Jahres-Strategie legt der EDSB dar, wie er diesen Auftrag auf verantwortungsvolle Weise zu erfüllen gedenkt.*

*Diese Stellungnahme steht im Zusammenhang mit dem Auftrag des EDSB, die EU-Organe bezüglich der Auswirkungen ihrer Politik auf den Datenschutz zu beraten und eine verantwortliche Politikgestaltung zu fördern. Dies steht im Einklang mit Maßnahme 9 der Strategie des EDSB: „Förderung einer verantwortungsvollen und fundierten politischen Entscheidungsfindung“.*

## Zusammenfassung

Die Verarbeitung personenbezogener Daten ist für webbasierte Dienste unverzichtbar. In der Strategie der EU für einen digitalen Binnenmarkt wird das Potenzial datengestützter Technologien und Dienste als Katalysator für das Wirtschaftswachstum anerkannt. Diese über das Internet erbrachten Dienste sind mittlerweile von einem häufig verdeckt stattfindenden Tracking von Personen abhängig, deren Art und Umfang dieser Verfolgung in aller Regel nicht bewusst sind. Die Unternehmen, die auf diesen Märkten eine beherrschende Stellung innehaben, sind unter Umständen in der Lage, neue Marktteilnehmer vom Wettbewerb um Faktoren, die den Rechten und Interessen des Einzelnen zugutekommen könnten, auszuschließen und unlautere Geschäftsbedingungen durchzusetzen, die eine missbräuchliche Ausbeutung der Verbraucher bewirken. Das offenkundig zunehmende Ungleichgewicht zwischen den Anbietern webbasierter Dienste und den Verbrauchern kann unter Umständen zu einer Einschränkung der Wahlfreiheit, der Innovationskraft und der Qualität der Garantien für den Schutz der Privatsphäre führen. Dieses Ungleichgewicht ist auch geeignet, den effektiven Preis – in Form einer Offenlegung personenbezogener Daten – weit über das auf vollständig wettbewerbsbestimmten Märkten zu erwartende Niveau anzuheben.

Im Jahr 2014 hat der EDSB eine vorläufige Stellungnahme zu Privatsphäre und Wettbewerbsfähigkeit im Zeitalter von Big Data vorgelegt. Wir haben festgestellt, dass die EU-Rechtsvorschriften zum Daten- und Verbraucherschutz sowie zur Durchsetzung des Kartellrechts und zur Fusionskontrolle ungeachtet offensichtlicher Synergieeffekte, beispielsweise im Hinblick auf Transparenz, Rechenschaftspflicht, Wahlfreiheit und die allgemeine Wohlfahrt, tendenziell eher unabhängig voneinander zur Anwendung kommen. Daher haben wir eine Debatte über einen holistischeren Ansatz für die Umsetzung der Ziele und Standards der EU in die Wege geleitet. Diese neue Stellungnahme basiert auf der Auffassung, dass die Strategie für einen digitalen Binnenmarkt eine Chance für einen kohärenten Ansatz bietet. Sie stellt eine Aktualisierung der vorläufigen Stellungnahme aus dem Jahr 2014 dar und beinhaltet einige praktische Empfehlungen an die EU-Organe im Hinblick auf mögliche Lösungsstrategien. Zudem wird die wachsende Besorgnis thematisiert, dass die Konzentration auf den digitalen Märkten den Interessen des Einzelnen als betroffene Person und als Verbraucher schaden könnte.

Die Organe und Einrichtungen der EU sowie die einzelstaatlichen Behörden müssen bei der Umsetzung des EU-Rechts die in der Charta der Grundrechte der EU verankerten Rechte und Freiheiten wahren. Mehrere dieser Bestimmungen, wie beispielsweise das Recht auf Privatsphäre und den Schutz personenbezogener Daten, die Freiheit der Meinungsäußerung und das Recht auf Nichtdiskriminierung, werden durch die gegenwärtig im Cyberspace geltenden normativen Verhaltensregeln und Standards in Frage gestellt. Die EU verfügt bereits über die erforderlichen Instrumente, um gegen Marktverzerrungen vorzugehen, die den Interessen des Einzelnen und der Gesellschaft insgesamt zuwiderlaufen. Einige der auf den digitalen Märkten üblichen Praktiken sind geeignet, gegen zwei oder mehr der geltenden Rechtsrahmen zu verstoßen, die sämtlich auf dem Begriff der „Fairness“ basieren. Wie die Autoren einiger der in den letzten Monaten vorgelegten Studien fordern auch wir eine Intensivierung des Dialogs, das Lernen aus Erfahrungen und eine Zusammenarbeit zwischen den für die Aufstellung der Verhaltensregeln im digitalen Umfeld zuständigen Aufsichtsbehörden. Darüber hinaus weisen wir nachdrücklich auf die Notwendigkeit hin, dass die EU sowohl online als auch offline Bedingungen schafft, in denen die in der Charta garantierten Rechte und Freiheiten gewahrt bleiben.

Daher wird in dieser Stellungnahme empfohlen, ein Clearinghaus für den digitalen Sektor zu schaffen, das die Aufgabe hat, innerhalb der EU Rechtsvorschriften im digitalen Sektor durchzusetzen. In diesem freiwilligen Netz sollen Aufsichtsbehörden auf freiwilliger Basis und im Rahmen ihrer jeweiligen Zuständigkeiten Informationen über mögliches missbräuchliches Verhalten im digitalen Ökosystem und die wirksamsten Optionen austauschen, um dagegen vorzugehen. Ergänzend dazu sollten Leitlinien zur kohärenten Anwendung der Vorschriften zum Schutz des Einzelnen durch die Aufsichtsbehörden bereitgestellt werden. Darüber hinaus empfehlen wir, dass die Organe der EU gemeinsam mit Sachverständigen die Möglichkeit der Schaffung eines gemeinsamen Raums im Internet prüfen, in dem Personen entsprechend den Bestimmungen der Charta trackingfrei interagieren können. Schließlich empfehlen wir die Aktualisierung der Regelungen über die Anwendung von Fusionskontrollen durch die Behörden, um den Schutz der Privatsphäre im Internet, der personenbezogenen Daten und der Freiheit der Meinungsäußerung zu verstärken.

# INHALT

<b>I. ERÖFFNUNG DER DEBATTE .....</b>	<b>6</b>
1. HINTERGRUND UND AUFBAU DIESER STELLUNGNAHME.....	6
2. UMSETZUNG DER ANALYSEERGEBNISSE IN PRAKTISCHES HANDELN .....	6
3. STRATEGISCHE BEDEUTUNG DIESER THEMATIK FÜR DIE DATENSCHUTZBEHÖRDEN ...	6
4. DER „WERT“ PERSONENBEZOGENER DATEN AUF DIGITALEN MÄRKTEN .....	7
<b>II. MACHT UND RECHENSCHAFTSPFLICHT .....</b>	<b>9</b>
1. ANPASSBARE RECHTLICHE VERPFLICHTUNGEN.....	9
2. KONZENTRATION VON MARKT- UND INFORMATIONSMACHT .....	9
<b>III. VERFÜGBARE SYNERGIEN .....</b>	<b>10</b>
1. GEMEINSAME ZIELE, ABER BEGRENZTE ZUSAMMENARBEIT .....	10
2. GESONDERTE, ABER MITEINANDER VERBUNDENE RECHTLICHE ZUSTÄNDIGKEITEN..	11
3. MÖGLICHKEITEN DER ZUSAMMENARBEIT .....	13
<b>IV. FÖRDERUNG DES DATENSCHUTZES UND VON TECHNOLOGIEN ZUM SCHUTZ DER PRIVATSPHÄRE ALS WETTBEWERBSVORTEIL.....</b>	<b>15</b>
1. VERTRAUEN UND TRACKING .....	15
2. PRIVATSPHÄRE ALS QUALITÄTSMERKMAL, DAS DEN WAHREN PREIS „UNENTGELTLICHER“ LEISTUNGEN BESTIMMT .....	16
3. UNGLEICHGEWICHTE BEI DIGITALEN TRANSAKTIONEN .....	16
4. EIN SCHWACHER MARKT FÜR DIENSTLEISTUNGEN ZUM SCHUTZ DER PRIVATSPHÄRE 17	
<b>V. EMPFEHLUNGEN: GESTALTUNG EINES AUF DEN WERTEN DER EU BASIERENDEN CYBERSPACE FÜR DIE EU.....</b>	<b>17</b>
1. BESSERE BERÜCKSICHTIGUNG DER INTERESSEN DES EINZELNEN BEI BIG-DATA- FUSIONEN .....	18
2. CLEARINGHAUS FÜR DIE RECHTSDURCHSETZUNG IM DIGITALEN SEKTOR .....	18
3. EIN AUF DEN WERTEN DER EU BASIERENDER GEMEINSAMER RAUM IM INTERNET .....	20
<b>VI. SCHLUSSFOLGERUNG .....</b>	<b>20</b>
<b>Anmerkungen .....</b>	<b>22</b>

# I. ERÖFFNUNG DER DEBATTE

## 1. Hintergrund und Aufbau dieser Stellungnahme

In unserer 2014 vorgelegten vorläufigen Stellungnahme zum Thema „Privatsphäre und Wettbewerbsfähigkeit im Zeitalter von ‚Big Data‘“ (im Folgenden: „vorläufige Stellungnahme“) wurde ein Vergleich der in der EU geltenden Rechtsrahmen für die Bereiche Datenschutz, Wettbewerb und Verbraucherschutz vorgenommen und der Schluss gezogen, dass im Kontext digitaler Märkte einige Synergien zu beobachten sind.<sup>1</sup> Wir richteten einige vorläufige Empfehlungen an die Organe der EU, die im Anschluss an einen im Juni 2014 vom EDSB ausgerichteten Workshop<sup>2</sup> weiter präzisiert wurden. Diese Empfehlungen betrafen unter anderem die folgenden Maßnahmen:

1. Besseres Verständnis des **„Wertes“ personenbezogener Daten auf digitalen Märkten** und Prüfung von Konzepten für Marktanalysen, insbesondere bezüglich der als „unentgeltlich“ angebotenen webbasierten Dienste, mit einer retrospektiven oder Ex-post-Analyse der Wirkung von Durchsetzungsentscheidungen;
2. Überlegungen zu Möglichkeiten der **Förderung von Technologien zum Schutz der Privatsphäre als Wettbewerbsvorteil**;
3. Überprüfung der **EU-Rechtsvorschriften und deren Relevanz für die digitalen Märkte des 21. Jahrhunderts**;
4. Erwägung praktischer Schritte zur **Zusammenarbeit zwischen den Behörden**, einschließlich eines engeren Dialogs und gemeinsamer Untersuchungen.

## 2. Umsetzung der Analyseergebnisse in praktisches Handeln

In dieser Stellungnahme werden diese Themen weiter untersucht. Darüber hinaus leistet sie aber auch einen Beitrag zu einer Debatte, die seit 2014 von eher abstrakten rechtlichen Argumenten zu dringenderen Problemstellungen übergegangen ist. Konzentration und Monopolmacht bergen insbesondere auf digitalen Märkten nicht nur für die Wettbewerbsfähigkeit, sondern auch für die Privatsphäre und die Freiheit der Meinungsäußerung Probleme. In ihrer im Mai 2015 verabschiedeten Strategie für einen digitalen Binnenmarkt<sup>3</sup> bekundete die Europäische Kommission die Absicht, die Regelungen im digitalen Ökosystem stärker zu harmonisieren und dafür zu sorgen, dass Europa in der globalen digitalen Wirtschaft die Führung übernimmt. Der Strategie zufolge spielt die Datenwirtschaft eine entscheidende Rolle für die Verbesserung der Wettbewerbsfähigkeit der EU, während Daten „Katalysatoren für Wirtschaftswachstum“ darstellen. Diese Stellungnahme ist das jüngste Ergebnis der kontinuierlichen Auseinandersetzung des EDSB mit dieser weit reichenden Strategie.<sup>4</sup> Sie soll über rein rechtliche Bemerkungen hinausgehen und praktische Maßnahmen aufzeigen, die eine kohärente Bewältigung dieser Herausforderungen im Zusammenhang mit der Rechtsdurchsetzung ermöglichen.<sup>5</sup>

## 3. Strategische Bedeutung dieser Thematik für die Datenschutzbehörden

Die Schnittstelle zwischen Wettbewerb und Privatsphäre sollte für alle unabhängigen Datenschutzbehörden ein zentrales, strategisches und langfristiges Thema darstellen. Personenbezogene Daten waren von zentraler Bedeutung für die Entwicklung digitaler Märkte, auf denen in einigen Fällen Dienstleistungen erbracht werden, die inzwischen als wesentlich betrachtet werden können. Wie wir bereits in einer früheren Stellungnahme<sup>6</sup> vorgebracht haben, stellen die rasche Entwicklung von auf personenbezogenen Daten basierenden Technologien

sowie die durch sie möglich gewordenen Datenverarbeitungsvorgänge, wie beispielsweise Big Data und das Internet der Dinge, für das Recht auf Datenschutz und einige andere Grundrechte eine bislang beispiellose Herausforderung dar. Einige der in der Charta verankerten klassischen Grundrechte – das Recht auf Privatsphäre (Artikel 7), die Freiheit der Meinungsäußerung (Artikel 11) und das Recht auf Nichtdiskriminierung (Artikel 21) – dienten ursprünglich dem Schutz vor staatlicher Einflussnahme. Inzwischen hat sich jedoch herausgestellt, dass im digitalen Zeitalter auch Garantien zum Schutz vor einer potenziellen Einflussnahme durch nichtstaatliche Einrichtungen und Einzelpersonen erforderlich sind. Dies führte (unter anderem) dazu, dass das Recht auf Datenschutz in Artikel 8 der Charta festgeschrieben wurde. In jüngster Zeit forderte der UN-Sonderberichterstatter über freie Meinungsäußerung die IKT-Branche auf, die Menschenrechte zu achten.<sup>7</sup>

Die Kommission stellte fest, dass Netzeffekte ein Merkmal digitaler Märkte sind.<sup>8</sup> Die gesellschaftlichen und beruflichen Kosten eines Verzichts auf webbasierte Dienste sind in vielen Fällen gestiegen, wobei keine Interoperabilität gegeben ist und die verfügbaren Optionen häufig nur einen geringen Schutz der Privatsphäre bieten. Wahlfreiheit ist ein Wettbewerbsparameter, jedoch ist es mittlerweile praktisch unmöglich, sich für eine trackingfreie Inanspruchnahme digitaler Dienste zu entscheiden.<sup>9</sup> Die offenkundige Zersplitterung des Internets nach Staatsgrenzen und die Aufteilung der Online-Erfahrung des Einzelnen in einige wenige „Walled Gardens“ (geschlossener Bereiche im Internet) stellen angesichts der Konzentration von Profit und Marktmacht eine Bedrohung für die Privatsphäre, den Schutz personenbezogener Daten, die Freiheit der Meinungsäußerung und des Freiraums für Innovationen dar.

Indessen könnte eine missbräuchliche Preisdiskriminierung – durch die Ausnutzung der Unterschiede hinsichtlich der erkennbaren Preissensibilität der Verbraucher – eine Abschöpfung der Konsumentenrente und Profitsteigerungen zur Folge haben.<sup>10</sup> Jüngste Studien haben gezeigt, dass Algorithmen für maschinelles Lernen das Potenzial haben, künftig eine perfekte Preisdiskriminierung 1. Grades zu ermöglichen, wobei Unternehmen für jeden einzelnen Verbraucher ein eigenes Marktsegment festlegen und ihm den Preis abverlangen, den er zu zahlen bereit ist. In naher Zukunft könnte es die Technologie Unternehmen auf digitalen Märkten erlauben, im Rahmen stillschweigender Absprachen mithilfe von Daten und selbstlernenden Algorithmen Preise festzusetzen.<sup>11</sup> Wirtschaftlich betrachtet könnte dies dazu führen, dass zwar eine Gewinnmaximierung, aber keine Verbraucherwohlfahrt erzielt wird, was ganz offensichtlich negative Auswirkungen auf die Grundrechte hätte. Datenschutz- und andere zuständige Behörden werden hier wachsam sein müssen.

#### **4. Der „Wert“ personenbezogener Daten auf digitalen Märkten**

Seit 2014 konzentrierten sich zahlreiche Debatten auf den „Wert“ von Big Data und die Frage, in welchem Maße diese mit personenbezogenen Daten gleichzusetzen sind. Während in zahlreichen Big-Data-Anwendungen Sachverhaltsdaten verarbeitet werden, wie beispielsweise Daten über das Wetter oder maschinelle Prozesse, nutzen Unternehmen und Behörden in zunehmendem Maße gewaltige Mengen personenbezogener Informationen, um menschliches Verhalten zu verstehen, vorherzusagen und zu beeinflussen.<sup>12</sup> Die größten Anbieter webbasierter Dienste, zu denen mehrere der zehn größten Unternehmen der Welt zählen, verdanken ihren Erfolg der Quantität und Qualität der von ihnen kontrollierten personenbezogenen Daten sowie dem geistigen Eigentum, das erforderlich ist, um diese Daten zu analysieren und daraus einen Mehrwert zu schaffen.<sup>13</sup> Personenbezogene Informationen sind für Unternehmen zu einem Wettbewerbsfaktor geworden und werden als „Rohstoff für digitale

Geschäftsmodelle“ beschrieben, die für Produktverbesserungen und gezielte Werbemaßnahmen herangezogen werden.<sup>14</sup>

Mittlerweile werden personenbezogene Daten gemeinhin mit einer Währung verglichen, die verwendet wird, um Zugang zu Online-Diensten zu erhalten. Im Vorschlag der Kommission betreffend Verträge über digitale Inhalte wird sogar anerkannt, dass personenbezogene Daten unter Umständen als Zahlungsmittel verwendet werden.<sup>15</sup> Daten können direkt als Ware gehandelt werden oder in einer ergänzenden Funktion als Input für die Entwicklung individueller Nutzerprofile dienen.<sup>16</sup> „Mehrseitige“ digitale Plattformen, die von den meisten Menschen bei der Internetnutzung als Mittler verwendet werden, behandeln Personen und Organisationen als Anbieter von Ideen und Produkten, die mit anderen zusammengebracht werden sollen. Erfolgreiche datengestützte mehrseitige Plattformen sind gewachsen, indem sie „unentgeltliche“ Inhalte und/oder Dienstleistungen angeboten haben, um riesige Mengen personenbezogener Daten anzusammeln, die Aufschluss über die vergangenen, gegenwärtigen und sogar künftigen Gewohnheiten und Vorlieben des Einzelnen geben. Die Plattformen sind auf der einen Seite für zahlende Kunden – in aller Regel Werbetreibende – interessant, indem sie personenbezogene Daten zusammentragen und analysieren, die sie auf der anderen Seite von nicht zahlenden Kunden erheben. Damit verwischt sich die traditionelle Unterscheidung zwischen Verbraucher und Hersteller.<sup>17</sup>

Die kommerzielle Kontrolle von Daten könnte das fehlende Element sein, welches das bemerkenswerte Aufblähen des Marktwerts erfolgreicher Unternehmen im digitalen Sektor erklärt.<sup>18</sup> In unserer vorläufigen Stellungnahme haben wir den damaligen Vizepräsident der Europäischen Kommission, Joaquín Almunia, mit seiner Forderung nach einer umfassenden Sektoranalyse für alle unentgeltlichen digitalen Dienste zitiert.<sup>19</sup> Im Zuge der Definition relevanter Märkte und der Quantifizierung von Marktmacht tendieren die Wettbewerbsbehörden im Einzelfall dazu, den Schwerpunkt auf die „zahlende“ Seite zu legen, die bislang in der Regel mit jenen gleichgesetzt wird, die nach Werbemöglichkeiten suchen. Die andere, „nicht zahlende“ Seite wird indessen nicht berücksichtigt, weil sie schwer quantifizierbar und eher Gegenstand anderer Rechtsbereiche ist. Die Effizienz dieser Märkte wird aufgrund der asymmetrischen Informationsverteilung zwischen den Marktseiten in Frage gestellt.<sup>20</sup> Angesichts dieser Unsicherheit begrüßen wir die Aufgeschlossenheit der Wettbewerbskommissarin, die dafür plädiert, bei der Fusionskontrolle nicht nur den Unternehmensumsatz, sondern auch die Bedeutung von Daten zu berücksichtigen.<sup>21</sup>

In der EU können personenbezogene Informationen nicht lediglich als wirtschaftliche Bestandsgrößen betrachtet werden.<sup>22</sup> Nach der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte sind bei der Verarbeitung personenbezogener Daten Garantien vonnöten, um die Wahrung des Rechts des Einzelnen auf Achtung des Privatlebens, Freiheit der Meinungsäußerung und Versammlungsfreiheit zu gewährleisten.<sup>23</sup> Des Weiteren ist das Recht auf den Schutz personenbezogener Daten in Artikel 8 der EU-Charta und Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) ausdrücklich verankert. Infolgedessen beinhaltet die im Jahr 2016 verabschiedete Datenschutz-Grundverordnung spezifische Garantien, die dazu beitragen könnten, Marktungleichgewichte im digitalen Sektor auszugleichen: Die Datenschutzbehörden müssen den Grundsatz der Datenminimierung durchsetzen, nach dem personenbezogene Informationen nur verarbeitet werden dürfen, wenn sie „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt“<sup>24</sup> sind. Darüber hinaus müssen sie dafür sorgen, dass das Recht des Einzelnen auf Informationen über die in die automatisierte Entscheidungsfindung einschließlich Profiling involvierte Logik gewahrt bleibt.<sup>25</sup> Des Weiteren sollten Daten- und Verbraucherschutzbehörden bereit und in der Lage sein, Wettbewerbsbehörden in Fusionsfällen im digitalen Sektor zu informieren und zu beraten,

wenn Anlass zu der Vermutung besteht, dass sich die betreffende Transaktion zum Nachteil von Personen auswirken könnte.

## **II. MACHT UND RECHENSCHAFTSPFLICHT**

### **1. Anpassbare rechtliche Verpflichtungen**

Die Rechtsvorschriften über den Datenschutz, den Schutz der Privatsphäre (Vertraulichkeit der Kommunikation) und den Verbraucherschutz wurden kürzlich oder werden derzeit überarbeitet, um den Schutz der Rechte des Einzelnen wirksamer in der neuen digitalen Realität zu verankern.<sup>26</sup> Eine der wichtigsten Neuerungen der neuen Datenschutz-Grundverordnung ist die Einbeziehung des Grundsatzes der Rechenschaftspflicht, der im Wettbewerbsrecht bereits einen festen Platz hat, im Datenschutzrecht jedoch relativ neu ist. Diesem Grundsatz zufolge müssen Datenschutzpflichten unterliegende Organisationen nachweisen können, dass die erforderlichen Maßnahmen ergriffen wurden, um die Einhaltung der Vorschriften zu gewährleisten, wobei die Datenschutzbehörden nur eine Kontrollfunktion wahrnehmen und insbesondere dann tätig werden, wenn Anhaltspunkte für einen Verstoß vorliegen. Die Verpflichtungen in jedem dieser Bereiche sind anpassbar: Wenn Unternehmen beispielsweise mehr Marktmacht (von Belang für die Wettbewerbsbehörden) oder eine stärkere Vertragsposition (Verbraucherschutz) innehaben oder für mit einem höheren Risiko verbundene Datenverarbeitungsvorgänge verantwortlich sind (Datenschutz), müssen sie bei den im Hinblick auf die Einhaltung der Vorschriften ergriffenen Maßnahmen größere Sorgfalt walten lassen.

Allerdings haben wir in vorangegangenen Stellungnahmen darauf hingewiesen, dass wirksame Rechtsvorschriften zwar notwendig, aber keineswegs ausreichend sind, um eine Kultur der Rechenschaftspflicht zu schaffen. Dies gilt auch für Märkte, auf denen das Verhalten der Akteure dem Einzelnen und der Gesellschaft insgesamt schaden kann und eine zunehmende Konzentration von Marktmacht zu beobachten ist. Häufig hinkt die Regulierung den technologischen und Marktentwicklungen hinterher; es entstehen innovative und dynamische Dienste, welche die etablierten Anbieter in Bedrängnis bringen, indem sie den Bedarf der Verbraucher effizienter decken. Die Anwendung von Vorschriften auf diese bahnbrechenden Dienste wird oft angefochten und muss gerichtlich geklärt werden.<sup>27</sup>

### **2. Konzentration von Markt- und Informationsmacht**

Im Jahr 2014 wurde bei einem Workshop des EDSB vorgebracht, dass auf von Big Data geprägten Märkten „Verbundvorteile“ und Konzentration letztendlich zur Entstehung von „Winner-takes-all-Situationen“ und Quasimonopolen führen, die aufgrund der absoluten „Dauerhaftigkeit“ ihrer digitalen Vermögenswerte zunehmende Skalenerträge erzielen.<sup>28</sup> In den letzten Jahren haben Zusammenschlüsse auf den digitalen Märkten den Wettbewerb für zahlreiche Dienstleistungen eingeschränkt, sodass die größten Unternehmen ihre marktbeherrschende Stellung seit mittlerweile mehr als einem Jahrzehnt behaupten können und somit den flüchtigen Charakter dieser Märkte Lügen strafen. Man geht davon aus, dass die herkömmlichen Ansätze nicht geeignet sind, die Gewinne auf einem normalen Niveau zu halten, was dazu führt, dass die Verbraucher überhöhte Preise bezahlen müssen.<sup>29</sup> Die wenigen nach Fusionen vorgenommenen Ex-post-Bewertungen belegen, dass die meisten Fusionen Preissteigerungen nach sich ziehen.<sup>30</sup> Zwar verdanken die marktbeherrschenden Unternehmen auf digitalen Märkten ihren Erfolg der Qualität ihrer Produkte, jedoch sind Zusammenschlüsse offenbar geeignet, im Laufe der Zeit einen Anstieg der Preise und Gewinne sowie einen Rückgang der Dienstleistungs- und Innovationsqualität zu bewirken.

Die größten Unternehmen im digitalen Sektor haben erhebliche Macht über die Kommunikation und Kontrolle über den Zugang zu Internetinhalten, auch wenn den Behörden offenbar die Handhabe für die Bestimmung ihrer „Marktmacht“ im herkömmlichen Sinne fehlt.<sup>31</sup> Heutzutage greifen die meisten Menschen über soziale Medien auf Nachrichten zu, wobei die Algorithmen der webbasierten Dienste anhand der Nutzerprofile festlegen, welche Inhalte dem Einzelnen präsentiert werden. Diesbezüglich werden zunehmend Bedenken laut, dass die Online-Erfahrung gefiltert und sich letztlich in einer Reihe von Echokammern abspielt.<sup>32</sup> Zudem sind Zusammenschlüsse auf digitalen Märkten kaum geeignet, den im EU-Recht verankerten Grundsatz der Datenminimierung zu stärken – was angesichts der Menge der verarbeiteten personenbezogenen Daten als Effizienzgewinn betrachtet werden könnte. Stattdessen haben Zusammenschlüsse dazu geführt, dass mehr personenbezogene Daten erhoben und miteinander verknüpft werden, wobei im Hinblick auf die Transparenz der Datennutzungsbedingungen keine Verbesserungen erkennbar sind.

Die Bedenken hinsichtlich Monopolmacht einerseits und Informationsmacht andererseits laufen somit zusammen, so wie Ende des 19. Jahrhunderts Fusionskontrolle und Menschenrechte in Europa und den Vereinigten Staaten zu einem gemeinsamen Anliegen der öffentlichen Ordnung wurden. Mächtige Organisationen haben das Potenzial, die Qualität der Privatsphäre und Freiheit der Nutzer digitaler Dienstleistungen einzuschränken oder effektiv als Zensoren von Online-Inhalten zu fungieren, selbst wenn sie diese Macht bislang nicht uneingeschränkt ausüben.<sup>33</sup> Seit der Veröffentlichung unserer vorläufigen Stellungnahme richten politische Entscheidungsträger größeres Augenmerk auf die Art der digitalen Transaktionen, für die kein Geld, sondern die Offenlegung personenbezogener Informationen verlangt wird, insbesondere wenn die Verarbeitung personenbezogener Daten für die Erbringung der betreffenden Dienstleistung nicht erforderlich ist.<sup>34</sup>

### III. VERFÜGBARE SYNERGIEN

#### 1. Gemeinsame Ziele, aber begrenzte Zusammenarbeit

Wie wir bereits festgestellt haben, zielt das Datenschutz-, Wettbewerbs- und Verbraucherrecht der EU auf den Schutz und die Förderung der Wohlfahrt sowie auf die Schaffung eines europäischen Binnenmarktes ab.<sup>35</sup> In den Debatten der beiden letzten Jahre spielte insbesondere der Grundsatz der Fairness eine Rolle, der für jeden dieser Rechtsbereiche von großer Bedeutung und in den einschlägigen Artikeln der EU-Charta und des AEUV verankert ist:

- im Verbraucherrecht ist der Grundsatz der Fairness das wohl wichtigste Kriterium für rechtmäßige Geschäftspraktiken;
- die Verarbeitung personenbezogener Daten nach Treu und Glauben stellt neben Rechtmäßigkeit und Transparenz einen zentralen Grundsatz dar;
- das Wettbewerbsrecht lässt wettbewerbswidrige Vereinbarungen zu, die eine „angemessene[] Beteiligung der Verbraucher an dem entstehenden Gewinn“ gestatten, und definiert die missbräuchliche Ausnutzung einer beherrschenden Stellung unter anderem als die „Erzwingung von unangemessenen Einkaufs- oder Verkaufspreisen“.<sup>36</sup>

Ungeachtet dessen findet auf europäischer Ebene nach wie vor nur eine begrenzte Zusammenarbeit zwischen den Behörden statt.<sup>37</sup> In unserer vorläufigen Stellungnahme haben wir den Begriff der gemeinsamen Anliegen für den Verbraucher erörtert. Allerdings wurde der Begriff der „Verbraucherwohlfahrt“ bislang im Wettbewerbsrecht nicht eindeutig definiert. In der Regel wird er im Zusammenhang mit Fragen der Marktstruktur und wirtschaftlichen

Effizienz verwendet und bezieht sich nur indirekt auf einzelne Belange der Verbraucher, wie beispielsweise den Schutz der Privatsphäre.<sup>38</sup> Artikel 102 AEUV verbietet die missbräuchliche Ausnutzung einer beherrschenden Stellung in Form der „Erzwingung von unangemessenen Einkaufs- oder Verkaufspreisen oder sonstigen Geschäftsbedingungen“. Allerdings überlassen die Wettbewerbsbehörden in der Regel Maßnahmen gegen einen solchen Ausbeutungsmissbrauch den Verbraucherschutzbehörden, während diese ihrerseits zuweilen das Vorgehen gegen missbräuchliche Klauseln in Verbraucherverträgen den Datenschutzbehörden anheimstellen.<sup>39</sup>

In einigen Fällen haben Behörden auf nationaler Ebene bereits erfolgreich zusammengearbeitet:

- Im September 2014 erging eine vorläufige Entscheidung der französischen Wettbewerbsbehörde, der zufolge GDF Suez seine marktbeherrschende Stellung missbräuchlich ausgenutzt hat, indem das Unternehmen die personenbezogenen Daten, die es als staatlicher Monopolist erhoben hatte, nutzte, um auf einem offenen, nicht regulierten Markt für ein Gas-/Strom-Paket zu werben. Die Behörde wies GDF an, einen Teil seiner Kundendaten gegenüber seinen Wettbewerbern offenzulegen und zuvor seinen Kunden die Möglichkeit zu geben, dieser Offenlegung zu widersprechen;
- die Datenschutzbehörde des Vereinigten Königreichs beriet die nationale Wettbewerbsbehörde im August 2015 im Zusammenhang mit deren Vorschlag, die Haushalte, die seit mindestens drei Jahren ihren Stromanbieter nicht gewechselt hatten, aufzufordern, der Offenlegung ihrer Daten gegenüber anderen Anbietern zu widersprechen;
- im September 2015 verhängte die belgische Wettbewerbsbehörde gegen die Belgische Nationallotterie eine Geldbuße in Höhe von 1,9 Mio. EUR, weil diese personenbezogene Daten, die sie ebenfalls als staatlicher Monopolist erhoben hatte, für den wettbewerbswidrigen Zweck genutzt hatte, auf dem benachbarten Sportwettenmarkt für den kommerziellen Wettdienst „Scoore!“ zu werben. Nach Auffassung der Behörde stellte dies eine missbräuchliche Ausnutzung einer marktbeherrschenden Stellung dar, indem Informationen verwendet wurden, die von den Wettbewerbern nicht repliziert werden konnten;
- im Jahr 2016 leitete das Bundeskartellamt nach eingehender Konsultation von Datenschutzbeauftragten, Verbraucherschutzverbänden und Wettbewerbsbehörden anderer Mitgliedstaaten eine Untersuchung bezüglich der Datenschutzrichtlinien des auf dem Markt für soziale Netzwerke möglicherweise marktbeherrschenden Unternehmens Facebook ein.<sup>40</sup>

Insgesamt zeichnet sich jedoch im Hinblick auf die Durchsetzung der EU-Rechtsvorschriften ein recht zersplittertes Bild ab: Die zuständigen Behörden sprechen sich nicht unbedingt ab, wenn sie sich mit Fällen befassen, bei denen erhebliche materiellrechtliche Überschneidungen bestehen. Sinnvoll wären beispielsweise gemeinsame Sitzungen der jeweiligen Koordinierungsstellen auf EU-Ebene, d. h. der Artikel-29-Datenschutzgruppe, des Europäischen Wettbewerbsnetzes und des Netzes für die Zusammenarbeit im Verbraucherschutz.

## **2. Gesonderte, aber miteinander verbundene rechtliche Zuständigkeiten**

Die Aufsichtsbehörden stehen häufig unter großem Druck, wenn es darum geht, trotz begrenzter Ressourcen und zunehmender Arbeitsbelastung den Erwartungen der Öffentlichkeit zu entsprechen. Insofern ist es nur natürlich, wenn sie sich auf ihre eigenen Zuständigkeiten konzentrieren. Die Grenzen der jeweiligen Befugnisse und Zuständigkeiten der Behörden

müssen respektiert werden: Natürlich sollen und können diese nicht die in anderen Rechtsbereichen geltenden Gesetze durchsetzen.<sup>41</sup> Es gibt keinen Rechtsbereich, der im Hinblick auf alle Probleme greift, und es wäre unangemessen, in einem anderen Bereich nach Lösungen zu suchen, um die eigenen Defizite zu kompensieren. Die Behörden der einzelnen Rechtsbereiche verfügen nur über begrenzte Optionen. So können beispielsweise die für die Durchsetzung des Wettbewerbsrechts zuständigen Behörden lediglich gegen die missbräuchliche Ausnutzung einer marktbeherrschenden Stellung, Kartellverhalten und Fusionen vorgehen, die den Interessen der Verbraucher zuwiderlaufen, während missbräuchliche Nutzungsbedingungen nicht zwangsläufig unter das Kartellrecht fallen.

Seit der Veröffentlichung unserer vorläufigen Stellungnahme kam es zu einem wichtigen Zusammenschluss: WhatsApp, eine beliebte Messenger-App, die alle Kontakte des Nutzers scannt, aber die Nutzerdaten nicht vermarktet, wurde von Facebook übernommen, das bei der Datennutzung einen vollkommen anderen Ansatz verfolgt. Die US-amerikanische Federal Trade Commission forderte die Parteien auf, ihre Kunden über etwaige Änderungen ihrer Nutzungsbedingungen zu informieren und ihnen entsprechende Wahlmöglichkeiten einzuräumen. Die Europäische Kommission entschied in ihrer Eigenschaft als EU-Wettbewerbsbehörde, dass auf der Grundlage der Fusionskontrollverordnung vom Erwerber nicht verlangt werden könne, die von den WhatsApp-Kunden unterzeichnete Datenschutzvereinbarung zu respektieren.<sup>42</sup> Jeder dieser Ansätze implizierte jedoch, dass die Nutzer des Messenger-Dienstes die neuen Bedingungen akzeptieren mussten, um nicht von dessen Nutzung ausgeschlossen zu werden. Kürzlich veranlasste eine Änderung der Datenschutzbestimmungen des Messenger-Dienstes WhatsApp die Wettbewerbskommissarin, Fragen zu dem aus dem Zusammenschluss hervorgegangenen Unternehmen aufzuwerfen.<sup>43</sup> Im Falle künftiger, ähnlicher Zusammenschlüsse könnte eine kohärentere Reaktion der Wettbewerbs-, Verbraucher- und Datenschutzbehörden zu einem für die Verbraucher zufriedenstellenderen Ergebnis führen. Die Aufsichtsbehörden müssen bestens gerüstet sein, um sowohl Verhaltensweisen als auch Zusammenschlüsse zu antizipieren und zu verhindern, die dem Einzelnen schaden könnten.

Keiner dieser regulatorischen Zuständigkeitsbereiche ist von den anderen hermetisch zu trennen. Eine hohe Konzentration auf Märkten könnte den Schutz der Grundrechte selbst dann unterminieren, wenn die Kartellbehörden kein wettbewerbswidriges Verhalten feststellen. Der Rechtsprechung zufolge wird von den Behörden bereits erwartet, die wahrscheinlichen Anreize für den Missbrauch einer marktbeherrschenden Stellung im Nachgang zu einem Zusammenschluss zu berücksichtigen.<sup>44</sup> Im Zuge der Durchsetzung der EU-Wettbewerbsvorschriften wurden in der Vergangenheit auch spezifischere politische Zielsetzungen verfolgt, wie beispielsweise die Deregulierung des Telekommunikationsmarktes.<sup>45</sup> Artikel 21 Absatz 4 der Fusionskontrollverordnung sieht konkret vor, dass die Mitgliedstaaten zusätzliche Kontrollen durchführen, um die Medienvielfalt zu schützen. Damit wird der Sorge Rechnung getragen, dass eine Konzentration in der Medienbranche die redaktionelle Unabhängigkeit und die Freiheit der Meinungsäußerung, wie sie in Artikel 11 der Charta verankert sind, beeinträchtigen könnte.<sup>46</sup>

„Selbst wenn sie anderen Zielen dienen, können Belange des Datenschutzes im Rahmen des Wettbewerbsrechts nicht einfach aufgrund ihrer Natur außer Acht gelassen werden“, heißt es in einem gemeinsamen Bericht der französischen und der deutschen Wettbewerbsbehörde zum Thema Wettbewerbsrecht und Daten, der im Mai 2016 veröffentlicht wurde.<sup>47</sup> Die Datenschutzbehörden können helfen, die Frage zu beleuchten, inwiefern und in welchem Maße die Kontrolle über personenbezogene Daten für die auf den Märkten aktiven Unternehmen von entscheidender Bedeutung ist. Die in den letzten Jahren ausführlich erörterten Synergien zwischen den Rechtsbereichen könnten Anlass für eine engere Zusammenarbeit zwischen den Behörden sein. Dies gilt insbesondere, wenn es diesbezüglich weder Vorgaben noch eine

Rechtsprechung gibt. Es geht nicht darum, einen anderen Rechtsbereich zu „instrumentalisieren“, sondern vielmehr um eine Synchronisierung der Politiken und Durchsetzungsmaßnahmen der EU, die einen Mehrwert schafft, wenn eine Aufsichtsbehörde nicht über die für eine Untersuchung erforderliche Erfahrung oder rechtliche Zuständigkeit verfügt.

### 3. Möglichkeiten der Zusammenarbeit

Die Strategie für einen digitalen Binnenmarkt beinhaltet zahlreiche vielversprechende Vorschläge für eine Verbesserung der Regelungsrahmen des Verbraucher- und Datenschutzes. Jedoch könnte die Strategie aufgewertet werden, indem ein Mechanismus für eine kohärente Durchsetzung der Verpflichtungen im Zusammenhang mit den Rechten und Interessen des Einzelnen in den verschiedenen Bereichen des EU-Rechts geschaffen wird.<sup>48</sup> Aus der Grundrechtsperspektive sollte im Rahmen der Strategie auch die Frage berücksichtigt werden, wie die meisten Menschen heute mit dem Internet interagieren: Ihre täglich genutzten webbasierten Dienste sind von einer zunehmend granularen Überwachung der Nutzer durch die Anbieter dieser Dienste abhängig, was häufig in Kontrast zu der Intransparenz steht, mit der eben diese Anbieter personenbezogene Daten verarbeiten (Black-Box-Phänomen).

In ihrer kürzlich vorgelegten Mitteilung zu Online-Plattformen erkennt die Kommission an, dass der grenzüberschreitende Charakter der Plattformen eine „gute Zusammenarbeit der zuständigen Behörden“ erfordert.<sup>49</sup> In ihrer Entschließung aus dem Jahr 2016 gingen die europäischen Datenschutzbehörden einen Schritt weiter und forderten „einen verstärkten Dialog und Informationsaustausch mit anderen Aufsichtsbehörden, die für den Schutz der Rechte und Interessen des Einzelnen in der digitalen Gesellschaft und Wirtschaft verantwortlich sind“, wobei sie die Bemühungen um die Intensivierung der Synergien zwischen den Rechtsrahmen für die Bereiche Verbraucherschutz, Wettbewerb und Datenschutz anerkannten.<sup>50</sup> Im Sinne der Grundsätze der Good Governance und der loyalen Zusammenarbeit sollten die Datenschutzbehörden in jedem Falle mit den für andere Politikbereiche zuständigen EU-Agenturen und nationalen Aufsichtsbehörden kooperieren.<sup>51</sup> Eine Arbeitsgruppe der Gemeinsamen Forschungsstelle der Kommission regte die Einrichtung einer spezialisierten Agentur an, die zum einen die Aufsichtsbehörden in fachlicher Hinsicht bei der Untersuchung von den digitalen Markt betreffenden Fällen unterstützen und zum anderen die Einhaltung der Rechtsvorschriften durch Online-Plattformen überwachen soll, um die „Kohärenz zwischen den Aufsichtsbehörden in ihren jeweiligen Zuständigkeitsbereichen“ zu verbessern.<sup>52</sup>

Ein gewinnbringendes Zusammenwirken der Aufsichtsbehörden wäre beispielsweise in den folgenden Bereichen denkbar:

- Untersuchung der längerfristigen Folgen von Zusammenschlüssen auf dem digitalen Markt – wie beispielsweise von Facebook und WhatsApp – für den Verbraucher und Klärung der Frage, ob die zum Zeitpunkt des Zusammenschlusses getätigten Zusagen oder Erklärungen der fusionierenden Parteien anschließend eingehalten werden;
- alle Fälle, in denen missbräuchliche Geschäftsbedingungen und Datennutzungsrichtlinien im Spiel sind, bieten sich ganz offensichtlich für eine Zusammenarbeit zwischen Datenschutz- und Verbraucherschutzbehörden an; werden diese Bedingungen von einem marktbeherrschenden Unternehmen angewendet, empfiehlt sich auch die Einbeziehung der Wettbewerbsbehörden;
- Fälle, in denen das Vorgehen marktbeherrschender Unternehmen geeignet ist, den Interessen der Verbraucher zu schaden oder datenschutzfreundliche Wettbewerber auszuschließen, wären ebenfalls hervorragende Gelegenheiten für einen Dialog

zwischen Wettbewerbs- und Verbraucherschutzbehörden und/oder Datenschutzbehörden: So hat beispielsweise ein Start-up eine Beschwerde gegen das auf dem Markt für mobile Betriebssysteme mutmaßlich beherrschende Unternehmen eingereicht, weil dieses eine App aus seinem App-Store ausgeschlossen hatte, die es den Nutzern ermöglicht, Dienste von Drittanbietern zu ermitteln und zu blockieren, die ihr Surfverhalten aufzeichnen oder möglicherweise Schadprogramme freisetzen.<sup>53</sup>

Unserer Auffassung nach bietet Artikel 80 der Datenschutz-Grundverordnung eine wichtige Gelegenheit für eine kollektive Rechtsdurchsetzung. Die Mitgliedstaaten sollten diese Bestimmung über kollektive Rechtsbehelfe anwenden, ohne dass von einer betroffenen Person ein spezifischer Auftrag vorliegen muss. Interessenverbände haben bereits begonnen, auf der Grundlage sowohl von Verbraucherschutz- als auch von Datenschutzbestimmungen Klagen zu erheben:

- UFC-Que Choisir und der Verbraucherzentrale Bundesverband (VZBV) haben gegen Betreiber sozialer Medien und Anbieter von Online-Diensten Klagen wegen missbräuchlicher Vertragsbedingungen, unlauterer Geschäftspraktiken und Verstößen gegen Datenschutzvorschriften eingereicht;<sup>54</sup>
- der norwegische Verbraucherschutzrat hat eine Studie über die von sieben Anbietern von Cloud-Diensten verwendeten Standardbedingungen veröffentlicht, die einen vergleichenden Überblick über verschiedene Geschäftsbedingungen bietet und in diesem Zusammenhang auch Datenschutzrichtlinien berücksichtigt. Aufgrund dieser Studie wurde beim norwegischen Bürgerbeauftragten für Verbraucherfragen eine Beschwerde gegen Apple eingereicht, in der geltend gemacht wurde, dass die Geschäftsbedingungen des Unternehmens gegen norwegisches und europäisches Verbraucherrecht verstoßen. Apple sagte eine Änderung seiner Geschäftsbedingungen und insbesondere der Klausel zu, nach der dem Unternehmen ein einseitiges Recht zustand, die Vereinbarung jederzeit nach eigenem Ermessen und ohne Unterrichtung der Nutzer zu ändern;<sup>55</sup>
- eine österreichische Verbraucherschutzorganisation beanstandete die von Amazon seinen Kunden einseitig auferlegten Geschäftsbedingungen auf der Grundlage der Richtlinie über missbräuchliche Klauseln in Verbraucherverträgen und der Datenschutz-Richtlinie. (Im August entschied der EuGH über die ihm vorgelegten Rechtsfragen.<sup>56</sup>)

Mittlerweile stellen die kollektive Rechtsdurchsetzung und die Beseitigung der „regulatorischen Fragmentierung“ dringende Anliegen dar, die auch von der Europäischen Kommission anerkannt werden. So forderte Kommissionspräsident Juncker zu Beginn seiner Amtszeit, die Kommission müsse das Schubladendenken aufbrechen. Auch der Europäische Verbraucherverband (BEUC) äußerte sich entsprechend.<sup>57</sup> Nun ist der Moment gekommen, um diese theoretischen Synergien in positives Handeln umzusetzen.

## IV. FÖRDERUNG DES DATENSCHUTZES UND VON TECHNOLOGIEN ZUM SCHUTZ DER PRIVATSPHÄRE ALS WETTBEWERBSVORTEIL

### 1. Vertrauen und Tracking

Das mangelnde Vertrauen der Verbraucher und ihre Wahrnehmung, kaum Kontrolle über die Vorgänge in Online-Umgebungen zu haben, stellen ein gemeinhin anerkanntes Problem dar.<sup>58</sup> Im Jahr 2015 wurden im Rahmen des Projekts „Ranking Digital Rights“ der New America Foundation viele der größten Unternehmen der Technologiebranche befragt. Dabei wurde festgestellt, dass sie alle die grundlegenden Standards des Datenschutzes und der Zensur missachteten, indem sie es beispielsweise versäumten, die Nutzer über die Bearbeitung oder Löschung ihrer Inhalte zu unterrichten, oder private Inhalte unzureichend verschlüsselten.<sup>59</sup> Daher haben wir nachdrücklich gefordert, dass die EU Anstrengungen unternimmt, um dieses Vertrauensdefizit zu beheben, indem sie sich für Rechenschaftspflicht und transparente Geschäftsmodelle, Wahlfreiheit, Datenübertragbarkeit, Nutzerkontrolle und wirksame Rechtsbehelfe bei Rechtsverstößen einsetzt. Kürzlich sprachen wir in unserer Antwort auf die jüngste Konsultation zur Reform der Datenschutzrichtlinie für elektronische Kommunikation gegenüber der Kommission folgende Empfehlungen aus:<sup>60</sup>

1. Abgesehen von First-Party-Analysen sollte bei keiner Form der elektronischen Kommunikation eine Rückverfolgung – durch Cookies, virtuelle Fingerabdrücke oder andere technologische Mittel – möglich sein, sofern nicht eine ohne Zwang gegebene Einwilligung erfolgt ist, die der Einzelne auf Wunsch einfach widerrufen kann;
2. jede Person sollte das Recht haben, selbst zu wählen, welche Inhalte Dritter zugelassen oder blockiert werden;
3. „Cookie Walls“, die faktisch den Zugang zu Websites verweigern, sofern der Nutzer nicht einem allgemeinen Tracking zustimmt, das nicht für die Leistung des Dienstes erforderlich ist, sollten verboten werden;
4. es sollte vorgeschrieben werden, dass Browser und andere Programme oder Betriebssysteme in ihren Voreinstellungen Zugriff auf Kontrollmechanismen bieten, über die der Nutzer einem Tracking zustimmen oder widersprechen kann.

Gemäß der wettbewerbsrechtlichen Rechtsprechung trägt ein marktbeherrschendes Unternehmen eine „besondere Verantwortung dafür ..., dass es durch sein Verhalten einen wirksamen und unverfälschten Wettbewerb auf dem gemeinsamen Markt nicht beeinträchtigt“<sup>61</sup>. Auf digitalen Märkten wurden Vorwürfe gegen marktbeherrschende Unternehmen laut, diese schlossen durch ihr Verhalten neue Marktteilnehmer aus, die datenschutzfreundlichere Leistungen anbieten, bei denen beispielsweise die Online-Aktivität der Nutzer nicht verfolgt wird, soweit dies nicht für die Erbringung der Leistungen erforderlich ist. Privatwirtschaftliche Initiativen wie der Do-Not-Track-Standard des World Wide Web Consortium, der eine versteckte Überwachung der Nutzer verhindern soll, konnten bislang keinen durchschlagenden Erfolg erzielen. Unter anderem darauf ist es zurückzuführen, dass sich Werbeblocker zu einer beliebten Taktik entwickelt haben, um gezielter Werbung aus dem Weg zu gehen. Dies wiederum hat zur Folge, dass die Betreiber Gegenmaßnahmen ergreifen und Scripts einsetzen, um Werbeblocker aufzuspüren und ihren Einsatz zu verhindern oder sogar zu verbieten.<sup>62</sup>

In der Tat stellt gezielte Werbung an sich kein grundrechtsrelevantes Problem dar. Von größerer Bedeutung für die Privatsphäre, den Datenschutz und die Wahrung anderer Grundrechte und

Freiheiten ist die Notwendigkeit, dem Einzelnen Optionen zugänglich zu machen, um die Kontrolle über seine personenbezogenen Daten zu behalten. Die Konzentration personenbezogener Daten in den Händen einer sinkenden Zahl von Unternehmen, die dem Einzelnen nur begrenzte oder keine Möglichkeiten einräumen, alle ihn betreffenden Daten auszumachen, war niemals die Absicht der Pioniere des Internets. Vielmehr hat der Erfinder des World Wide Web ein Projekt ins Leben gerufen, um diesen Trend umzukehren. Hierfür soll ein System dezentraler sozialer Anwendungen entwickelt werden, in dem jeder einzelne Nutzer kontrolliert, „wo, wie und an wen“ seine personenbezogenen Daten weitergegeben werden.<sup>63</sup>

## **2. Privatsphäre als Qualitätsmerkmal, das den wahren Preis „unentgeltlicher“ Leistungen bestimmt**

Die Qualität eines Produktes oder einer Dienstleistung ist ein Wettbewerbsparameter. In mehrseitigen Märkten ist sie „vielschichtig“ und „unklar“ und somit schwer zu ermitteln, spielt jedoch im Rahmen der Wettbewerbsanalyse nach wie vor eine wichtige Rolle.<sup>64</sup> Privatsphäre und die Standards für den Datenschutz und die Datensicherheit sind Teil dieses Parameters. Eine Einschränkung der von einem webbasierten Dienst gewährten Privatsphäre stellt einen Nachteil für den Verbraucher dar, der sowohl für die Durchsetzung der Wettbewerbsvorschriften als auch für den Verbraucherschutz relevant ist.<sup>65</sup> Im Rahmen mehrerer nationaler Untersuchungen zu sozialen Medien und anderen Online-Diensten wurden Fragen im Zusammenhang mit der Transparenz und Fairness der Geschäftsbedingungen einiger Online-Dienste aufgeworfen, wie beispielsweise bei der deutschen Untersuchung zur möglichen „missbräuchlichen Ausnutzung von Marktmacht unter Verletzung der Datenschutzbestimmungen“<sup>66</sup> durch Facebook.

Die Ermittlung der Fähigkeit eines Unternehmens, den Preis anzuheben, ist bei „unentgeltlichen“ Diensten problematisch, weil es derzeit keinen allgemeinen Standard für die Bemessung des tatsächlichen Preises solcher Angebote gibt. Die von auf Gewinnmaximierung ausgerichteten Unternehmen zum Nulltarif angebotenen Dienste sind jedoch für die Behörden ebenso relevant wie die zu einem anderen Preis angebotenen Dienste, wenn auch bis vor Kurzem diesbezüglich kaum Untersuchungen durchgeführt wurden. Dient die Extraktion von Informationen einem anderen Zweck als der Verbesserung der Qualität eines unentgeltlich angebotenen Produkts oder der Senkung der dafür anfallenden Kosten, stellen die Menge der extrahierten Informationen sowie die Werbeeinblendungen, die die Aufmerksamkeit der Verbraucher in Anspruch nehmen, in der Tat Kosten für sie dar. Das Angebot unentgeltlicher Dienste hat erhebliche Auswirkungen auf das Verhalten und die Nachfrage der Verbraucher, wobei sich diese ein subjektives und nicht unbedingt rationales Urteil über die ihnen im Hinblick auf ihre Aufmerksamkeit und Daten entstehenden Kosten sowie die Qualität des Produkts bilden. Die Rechtsdurchsetzung sollte darauf abzielen sicherzustellen, dass die Verbraucher die bestmögliche Qualität und Wahlfreiheit zu möglichst geringen Kosten in Form von Daten und Aufmerksamkeit erhalten, wenn es um unentgeltliche Dienste geht.<sup>67</sup>

## **3. Ungleichgewichte bei digitalen Transaktionen**

Wenn die Abschöpfung personenbezogener Daten wie oben erläutert in der digitalen Welt einen Näherungswert für den Preis darstellt, herrscht bei der Aufteilung der „digitalen Dividende“ auf Händler und Verbraucher, d. h. den für die Verarbeitung Verantwortlichen einerseits und die betroffenen Personen andererseits, ein größeres Ungleichgewicht denn je. Marktbeherrschende Plattformen sind in der Lage, Nutzer zu benachteiligen, indem sie das Wissen, das sie aus Daten beziehen, mit Monopolmacht und vertikaler Marktintegration verbinden. Im Rahmen der im Jahr 2012 durchgeführten koordinierten Ermittlung („Sweep“) der europäischen Verbraucherschutzbehörden zur Rechtsdurchsetzung wurden unlautere und irreführende Praktiken festgestellt.<sup>68</sup> Es ist fraglich, ob es fair sein kann, den Nutzern von

Online-Diensten Geschäftsbedingungen aufzuzwingen, deren Lektüre im Durchschnitt 25 Tage pro Jahr in Anspruch nehmen würde. Wettbewerb sollte den Verbrauchern in Form niedrigerer Preise, höherer Qualität und eines größeren Angebots zugutekommen.<sup>69</sup> Ohne Wettbewerb und ohne Wahlfreiheit der Verbraucher hat ein Monopolist jedoch keine Veranlassung, gute Dienstleistungen zu erbringen.<sup>70</sup>

Transparenz hinsichtlich der Verwendung der Daten ist notwendig, aber wenn es keine realistische Alternative gibt, führt sie schlichtweg zu einer „Friss-oder-stirb“-Situation der Nutzer. Diese Problematik ist beispielsweise im deutschen Facebook-Fall relevant.<sup>71</sup> Solche webbasierten Dienste sind durch eine Informationsasymmetrie gekennzeichnet: Einzelpersonen oder kleine Unternehmen verfügen nur über unzureichendes Hintergrundwissen bezüglich Preis und Qualität eines Produkts, während große Unternehmen auf preisrelevante Informationsströme und Risikomanagementprofile zurückgreifen können, um ihre Fähigkeit zu maximieren, die Konsumentenrente abzuschöpfen.<sup>72</sup> Datenschutz- und Verbraucherschutzbehörden sind gleichermaßen gut gerüstet, um Empfehlungen zu diesen Entwicklungen abzugeben.

#### **4. Ein schwacher Markt für Dienstleistungen zum Schutz der Privatsphäre**

Der Markt für Technologien zum Schutz der Privatsphäre – d. h. für Technologien, die darauf abzielen, die Verarbeitung personenbezogener Daten auf das erforderliche Mindestmaß zu beschränken, ohne die Funktionalität eines Produktes oder einer Dienstleistung zu beeinträchtigen – ist nach wie vor schwach.<sup>73</sup> Privatsphäre ist ein universelles menschliches Bedürfnis, auch wenn viele bereit sind, in den sozialen Medien persönliche Details preiszugeben, und der fehlende Wettbewerb um Privatsphäre stellt ein Marktversagen dar.<sup>74</sup> Mit der Datenschutz-Grundverordnung wurden nun Entwickler verpflichtet, den Grundsätzen des „Datenschutzes durch Technik“ und des „Datenschutzes durch datenschutzfreundliche Voreinstellungen“ Genüge zu tun. Das in der Datenschutz-Grundverordnung verankerte neue Recht auf Datenübertragbarkeit sollte, wenn es ordnungsgemäß umgesetzt und durchgesetzt wird, dazu beitragen, dass die Nutzer nicht mehr an bestimmte webbasierte Dienste gebunden sind. Des Weiteren haben wir erläutert, dass die gegenwärtig überprüften Regelungen zur Vertraulichkeit der Kommunikation – die Teil des Rechts auf Privatsphäre ist – nicht nur auf die herkömmliche Telekommunikation, sondern auf alle Formen der digitalen Kommunikation wirksam angewendet werden müssen.<sup>75</sup> Diese legislativen Entwicklungen bieten zwar Mindeststandards für den Schutz des Einzelnen, schaffen aber nicht notwendigerweise die Marktbedingungen, unter denen Privatsphäre und Freiheit der Meinungsäußerung zum Gegenstand des Wettbewerbs werden.<sup>76</sup> Darüber hinaus ist es notwendig, dass die Aufsichtsbehörden beim Einsatz der vorhandenen Instrumente verstärkt zusammenarbeiten, um diesen Wettbewerb zu befördern und gegen wettbewerbswidriges Verhalten vorzugehen, das Innovationen behindert oder die Privatsphäre und damit die Qualität eines Produkts beeinträchtigt.

### **V. EMPFEHLUNGEN: GESTALTUNG EINES AUF DEN WERTEN DER EU BASIERENDEN CYBERSPACE FÜR DIE EU**

Nach Artikel 51 der Charta achten die „Organe, Einrichtungen und sonstigen Stellen der Union unter Wahrung des Subsidiaritätsprinzips und ... die Mitgliedstaaten ausschließlich bei der Durchführung des Rechts der Union ... die Rechte, halten ... sich an die Grundsätze und fördern

... [die] Anwendung“ der Bestimmungen der Charta „entsprechend ihren jeweiligen Zuständigkeiten“.77 Des Weiteren verlangt der AEUV, dass die EU „auf die Kohärenz zwischen ihrer Politik und ihren Maßnahmen in den verschiedenen Bereichen“ achtet.78 Politiker und Behörden suchen nach Möglichkeiten, um die mit Big-Data-Konnektivität, hoher Rechenleistung sowie allgegenwärtigen und verzögerungsfreien Datenströmen verbundenen Vorteile einer möglichst breiten Öffentlichkeit zugänglich zu machen. Das Europäische Parlament forderte kürzlich, die EU müsse im Zuge der Ausarbeitung neuer Rechtsvorschriften gegen die Fragmentierung der Rechtsvorschriften vorgehen und im Hinblick auf die Umsetzung des EU-Rechts durch die Mitgliedstaaten auf ein hohes Maß an Kohärenz hinwirken.79 Die Organe der EU sollten mit gutem Beispiel vorangehen und für eine solche Kohärenz beim Schutz der in der Charta verankerten Grundrechte Sorge tragen. Hierfür müssen die auf EU-Ebene verfügbaren Instrumente eingesetzt werden, um die Bedingungen zu schaffen, unter denen diese Rechte und Freiheiten gedeihen können. Darüber hinaus sind gemeinsame Durchsetzungsmaßnahmen erforderlich, um die Synergien zwischen den relevanten Rechtsbereichen zu heben. Wir schlagen drei praktische Schritte vor, um die Realisierung dieser Zielsetzungen zu unterstützen.

## **1. Bessere Berücksichtigung der Interessen des Einzelnen bei Big-Data-Fusionen**

Bislang lag das Hauptaugenmerk der EU-Fusionskontrolle auf Unternehmen, die bestimmte Umsatzschwellen überschreiten, sofern sie nicht von den nationalen Behörden mit konkreten Fällen befasst wurde. Mittlerweile gibt es Anzeichen für eine stärkere Kontrolle geplanter Übernahmen weniger etablierter digitaler Unternehmen, die unter Umständen erhebliche Mengen personenbezogener Daten angehäuft haben, deren Geldwert noch ermittelt werden muss.80 Wir befürworten dies und würden empfehlen, das Fachwissen unabhängiger Datenschutzbehörden in Anspruch zu nehmen, um zu klären, wie die Bedeutung der Verbraucherwohlfahrt im Rahmen solcher Vorhaben bewertet werden kann.

Des Weiteren sollte die Fusionskontrollverordnung dahingehend ausgelegt und bei nächster Gelegenheit geändert werden, dass die in der EU-Charta verankerten Rechte auf Privatsphäre, Datenschutz und Freiheit der Meinungsäußerung im Internet ebenso geschützt werden wie gegenwärtig die Medienvielfalt. Die Mitgliedstaaten sollten die Möglichkeit erhalten, diese Rechte ebenfalls als „berechtigte Interessen“ zu schützen, „welche mit den allgemeinen Grundsätzen und den übrigen Bestimmungen des Gemeinschaftsrechts vereinbar sind“.81

## **2. Clearinghaus für die Rechtsdurchsetzung im digitalen Sektor**

Unsere Analyse führt uns zu dem Schluss, dass nun dringend eine kohärente Durchsetzung der digitalen Rechte in allen Rechtsbereichen erforderlich ist, die digitale Märkte berühren. In der EU kommt eine Reihe unterschiedlicher Rechtsinstrumente zur Anwendung, mit denen ähnliche Zielsetzungen verfolgt werden: Fairness, Marktintegration und Verbraucherwohlfahrt. Die Durchsetzung der wettbewerbsrechtlichen Vorschriften ist nicht nur aufgrund der hohen Geldbußen so wirksam, sondern auch weil sie Verhaltensweisen von Unternehmen und Organisationen unterbindet. Die neuen, verschärften Vorschriften zum Daten- und Verbraucherschutz könnten somit ebenso wie das Wettbewerbsrecht Veränderungen herbeiführen, beispielsweise beim Umgang mit personenbezogenen Daten, und damit Fairness und Verbraucherwohlfahrt insgesamt verbessern.

**Daher schlagen wir die Schaffung eines Clearinghauses<sup>82</sup> für den digitalen Sektor vor.** Dieses Clearinghaus bestünde in einem freiwilligen Netzwerk von Kontaktstellen der auf nationaler und EU-Ebene für die Regulierung des digitalen Sektors zuständigen Aufsichtsbehörden. Dabei könnten beispielsweise auch Behörden im Telekommunikationsbereich einbezogen werden, welche die Umsetzung der Vorschriften über die Vertraulichkeit der Kommunikation überwachen. Die Teilnahme an diesem Netzwerk wäre von zwei Kriterien abhängig:

1. **das gemeinsame Ziel**, sich gegenseitig in den jeweiligen Durchsetzungstätigkeiten zu unterstützen und das bestmögliche Ergebnis für die Rechte und die Wohlfahrt des Einzelnen zu erzielen, sei es als Verbraucher oder als betroffene Person;
2. **die Bereitschaft zum Austausch von Informationen und zur Zusammenarbeit** innerhalb der rechtlichen Zuständigkeiten und unter Wahrung der Vertraulichkeit von Untersuchungstätigkeiten.

Das Clearinghaus könnte die folgenden Aufgaben wahrnehmen:

1. Erörterung (jedoch nicht Festlegung) des am besten geeigneten Rechtsrahmens für die Untersuchung bestimmter Fälle oder Beschwerden, die digitale Dienste zum Gegenstand haben, insbesondere im Zusammenhang mit grenzübergreifenden Fällen, in denen möglicherweise gegen mehr als einen Rechtsrahmen verstoßen wird, und Ermittlung denkbarer koordinierter Aktionen oder Sensibilisierungsiniciativen auf europäischer Ebene, die geeignet wären, schädliche Praktiken zu unterbinden oder zu verhindern;
2. Heranziehung der Daten- und Verbraucherschutzvorschriften für die Festlegung relevanter „Schadentheorien“ für die Fusionskontrolle und Fälle von Ausbeutungsmissbrauch im Sinne des Wettbewerbsrechts gemäß Artikel 102 AEUV, um Orientierungshilfen zu erarbeiten, wie sie bereits für Fälle von Behinderungsmissbrauch verfügbar sind;<sup>83</sup>
3. Erörterung von Regulierungsmöglichkeiten für bestimmte Märkte, auf denen personenbezogene Daten einen entscheidenden Faktor darstellen, als wirksame Alternative zu möglicherweise innovationshemmenden Rechtsvorschriften für digitale Märkte;
4. Beurteilung der Auswirkungen der für die Lösung bestimmter Fälle vorgeschlagenen Sanktionen und Abhilfemaßnahmen auf die digitalen Rechte und Interessen des Einzelnen;
5. Ermittlung allgemeiner Synergien und Förderung der Zusammenarbeit zwischen den Durchsetzungsbehörden sowie des gegenseitigen Verständnisses der jeweils anwendbaren Rechtsrahmen, einschließlich einer Intensivierung der informellen und formellen Kontakte zwischen dem Europäischen Wettbewerbsnetz, dem Netz für die Zusammenarbeit im Verbraucherschutz und der Artikel-29-Datenschutzgruppe (die im Jahr 2018 durch den Europäischen Datenschutzausschuss ersetzt werden soll).

Das Clearinghaus für den digitalen Sektor könnte zu Beginn einige wenige Behörden umfassen, die bereit sind, sich auf den Austausch von Kontaktdaten und Informationen zu einigen, selbstverständlich im Rahmen ihrer Zuständigkeiten und unter Wahrung ihrer Handlungsfreiheit und Ermessensspielräume sowie der Vertraulichkeit ihrer Durchsetzungsverfahren. Der ESDB ist bereit, die Errichtung und Pflege dieses Netzwerks zu unterstützen und zu fördern.

### 3. Ein auf den Werten der EU basierender gemeinsamer Raum im Internet

Der Staat hat die positive Verpflichtung, die Achtung des Privatlebens zu gewährleisten; diese Verpflichtung reicht „bis in die Beziehungen zwischen den Einzelnen untereinander“ hinein.<sup>84</sup> Wir sind der Auffassung, dass die EU die gegenwärtige Tendenz zu einer Überwachung im Internet hinter sich lassen und die Schaffung eines gemeinsamen Raums in Betracht ziehen sollte, in dem Personen ohne Angst vor Tracking und sie betreffenden unlauteren Rückschlüssen interagieren können. Diesbezügliche Empfehlungen wurden in den letzten Jahren in mehreren Studien ausgesprochen.<sup>85</sup> So könnte dafür gesorgt werden, dass der Nutzer nicht länger nur die Wahl hat zwischen „unentgeltlichen“ Diensten, deren finanzielle Tragfähigkeit nur durch ein Tracking zu Werbezwecken gewährleistet werden kann, und kostenpflichtigen Diensten, denen die Nutzer mittlerweile eher aus dem Weg gehen: Privatsphäre ist kein Luxus, sondern ein universelles Recht, und sollte nicht nur jenen vorbehalten sein, die über die notwendigen Mittel verfügen, um dafür zu bezahlen. Dieser gemeinsame Raum ist von den „geschlossenen digitalen Räumen“ („*digital enclosures*“) zu unterscheiden, in denen sich die meisten Internetnutzer inzwischen bewegen und die von mehreren führenden Wissenschaftlern kritisiert wurden.<sup>86</sup> Er müsste als ein echter gemeinsamer Raum mit angemessenen Garantien gestaltet sein, in dem die Bestimmungen der EU-Charta uneingeschränkt gewahrt werden, einschließlich der in Artikel 52 Absatz 1 verankerten Bedingungen für jede Einschränkung der in der Charta anerkannten Rechte und Freiheiten.

Die Dienste, die beispielsweise im Rahmen der von zivilgesellschaftlichen Organisationen oder Entwicklern ins Leben gerufenen Initiativen bereits jetzt ohne Tracking und Profiling angeboten werden, könnten als Vorbild und Quelle für Erfahrungswerte herangezogen werden, um die neuen Konzepte voranzutreiben. Zugleich sollten die EU-Behörden die praktische Anwendung technischer Lösungen fördern, die dem ausdrücklichen Wunsch der Nutzer nach Schutz ihrer Privatsphäre nachkommen, indem sie beispielsweise klarstellen, wie der Do-Not-Track-Standard von W3C als Datenschutzinstrument einzusetzen ist. Zudem sollten sie untersuchen, wie die im Zuge der Reform des Datenschutzrahmens erweiterten Durchsetzungsbefugnisse genutzt werden können, um die Realisierung dieses Ziels zu unterstützen.

Wir werden eine Debatte mit der Europäischen Kommission und anderen EU-Organen in die Wege leiten und laden alle Interessengruppen ein, ihren Beitrag zu einer Vertiefung dieser Gespräche zu leisten.<sup>87</sup>

## VI. SCHLUSSFOLGERUNG

Die Menschenrechte wurden ursprünglich festgeschrieben, um den Einzelnen vor staatlicher Einflussnahme zu schützen. Die Fusionskontrolle hat ihre Wurzeln in dem politischen Willen, die missbräuchliche Ausnutzung von Monopolmacht zum Wohle der Gesellschaft insgesamt zu unterbinden. Die Verbraucherrechte wurden als Bollwerk gegen missbräuchliche Handelspraktiken konzipiert.

Die mit Big Data verbundenen Möglichkeiten im Hinblick auf die Steigerung von Produktivität und Konnektivität sollten mit Garantien zum Schutz der Sicherheit dieser Daten ausgestattet werden. Die EU hat in den letzten Jahren eine Vorreiterrolle übernommen und versucht, einen „Wettlauf“ um die Datenschutzstandards in der digitalen Arena anzufachen. Die Datenschutz-Grundverordnung schafft einen Maßstab für den Schutz personenbezogener Daten in der

digitalen Wirtschaft. Um eine digitale Wirtschaft und Gesellschaft zu gestalten, die auf den Werten der EU basiert, kann die EU mit den verfügbaren Instrumenten noch mehr tun, um dafür zu sorgen, dass Produkte und Dienstleistungen datenschutzfreundlich sind und die Wahrung der Grundrechte sicherstellen. Verbesserte Transparenz, ein fairer Umgang mit dem Einzelnen, wirksame Wahlfreiheit und die Gewährleistung, dass Modelle, die ohne Tracking auskommen, nicht vom Markt ausgeschlossen werden – alle diese Ziele sind vollständig kompatibel und ergänzen einander.

Die Strategie für einen digitalen Binnenmarkt bietet der EU die Chance für ein kohärentes Hinwirken auf diese Ziele. Die wirksame Durchsetzung der geltenden Vorschriften des EU-Rechts ist von größter Bedeutung. Wir sind überzeugt, dass das von uns empfohlene Clearinghaus für die Rechtsdurchsetzung im digitalen Sektor, ein holistischerer Ansatz im Hinblick auf die Konzentration sowie die Förderung eines auf den Werten der EU basierenden gemeinsamen Raums wichtige Schritte in die richtige Richtung darstellen würden. In dieser Zeit, in der weltweit Rechtsvorschriften zum Schutz von Daten und der Privatsphäre erlassen werden, sollte hier eine Plattform geschaffen werden, um Brücken zu anderen Regionen der Welt zu schlagen und eine Intensivierung des Dialogs sowie der Zusammenarbeit mit allen Ländern zu ermöglichen, die mit derselben digitalen Herausforderung konfrontiert sind.

Mit dieser Stellungnahme ist das letzte Wort in dieser Debatte noch nicht gesprochen. Der EDSB beabsichtigt, auch weiterhin Diskussionen anzuregen und seinen Beitrag dazu zu leisten, die Mauern niederzureißen, die den Schutz der Interessen und Rechte des Einzelnen behindern.

Brüssel, den 23. September 2016

Giovanni BUTTARELLI  
Europäischer Datenschutzbeauftragter

## Anmerkungen

<sup>1</sup> Vorläufige Stellungnahme des EDSB, *Privatsphäre und Wettbewerbsfähigkeit im Zeitalter von „Big Data“: das Zusammenspiel zwischen Datenschutz, Wettbewerbsrecht und Verbraucherschutz in der digitalen Wirtschaft*, März 2014.

<sup>2</sup> *Report of workshop on Privacy, Consumers, Competition and Big Data*, 2. Juni 2014; <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/consultation/Big%20data>.

<sup>3</sup> Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Strategie für einen digitalen Binnenmarkt für Europa, COM(2015) 192 final.

<sup>4</sup> Stellungnahme 7/2015 des EDSB, *Bewältigung der Herausforderungen in Verbindung mit Big Data*.

<sup>5</sup> Bestimmte fachliche Fragestellungen, die in der vorläufigen Stellungnahme im Zusammenhang mit der Wettbewerbsanalyse behandelt wurden, wie beispielsweise die Definition der Märkte und die Bedeutung von Daten als „wesentliche Einrichtung“, werden in der vorliegenden Stellungnahme nicht weiter vertieft. Stattdessen liegt der Schwerpunkt auf den wichtigsten Bereichen einer kohärenten Anwendung der Datenschutz-, Verbraucherschutz- und Wettbewerbsbestimmungen. Diese Aspekte könnten unter Umständen Gegenstand strukturierterer Gespräche zwischen den Aufsichtsbehörden sein, die wir befördern wollen.

<sup>6</sup> Stellungnahme 4/2015 des EDSB, *Der Weg zu einem neuen digitalen Ethos*.

<sup>7</sup> Bericht des Sonderberichterstatters über die Förderung und den Schutz des Rechts auf Meinungsfreiheit und freie Meinungsäußerung, David Kaye, 22. Mai 2015.

<sup>8</sup> Ocello, E., Sjodin, C. und Subocs, A. (2015), „What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU merger case“, in Europäische Kommission, *Competition merger brief*, Ausgabe 1/2015, S. 1 ff.

<sup>9</sup> Tim Berners Lee zufolge hat das Internet das Potenzial für einen hervorragenden Ausgleichsmechanismus, aber „nur, wenn wir das Recht auf Privatsphäre und die Freiheit der Meinungsäußerung ... fest darin verankern“; <http://webfoundation.org/2014/12/recognise-the-internet-as-a-human-right-says-sir-tim-berners-lee-as-he-launches-annual-web-index/> [abgerufen am 17. September 2016]. Siehe beispielsweise: Nissenbaum, H. und Howe, D., „Track me not: resisting surveillance in the web search“, in Julia Angwin, *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, 2014.

<sup>10</sup> Autorité de la Concurrence und Bundeskartellamt, *Competition Law and Data*, Mai 2016.

<sup>11</sup> Zur Aussicht von Preisalgorithmen, die letztendlich eine künstliche Intelligenz schaffen und wettbewerbswidrige sowie wahrscheinlich unethische Absprachen ermöglichen, siehe Ezrachi, A. und Stucke, M. E., *Artificial Intelligence & Collusion: When Computers Inhibit Competition*, in Oxford Legal Studies Research Paper Nr. 18/2015, 8. April 2015, University of Tennessee Legal Studies Research Paper Nr. 267.

<sup>12</sup> Siehe EDSB, *Bewältigung der Herausforderungen in Verbindung mit Big Data*.

<sup>13</sup> Financial Times Global 500.

<sup>14</sup> Monopolkommission, Sondergutachten, *Wettbewerbspolitik: Herausforderung digitale Märkte*, 2015, S. 57.

<sup>15</sup> Gemäß Artikel 3 Absatz 1 der von der Kommission vorgeschlagenen Richtlinie soll diese für Verträge gelten, auf deren Grundlage „der Verbraucher ... einen Preis zahlt oder aktiv eine andere Gegenleistung als Geld in Form personenbezogener oder anderer Daten erbringt“. Mit Artikel 3 Absatz 4 werden Verträge aus dem Anwendungsbereich der Richtlinie ausgeschlossen, bei denen der Anbieter vom Verbraucher lediglich ein Mindestmaß an personenbezogenen Daten verlangt, die „für die Erfüllung des Vertrags oder die Erfüllung rechtlicher Anforderungen unbedingt erforderlich [sind], und er diese Daten nicht in einer mit diesem Zweck nicht zu vereinbarenden Weise weiterverarbeitet“. Im Vorschlag der Kommission wird der Grundsatz akzeptiert, dass personenbezogene Daten als Zahlungsmittel fungieren können. Fragwürdig ist allerdings, dass zugleich Fälle ausgeschlossen werden, in denen der Anbieter personenbezogene Daten erhebt, „ohne dass der Verbraucher diese aktiv bereitstellt“: COM(2015) 634 final, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte.

<sup>16</sup> Costa-Cabral, F. und Lynskey, O., „The Internal and External Constraints of Data Protection on Competition Law in the EU“, in *LSE Law, Society and Economy Working Papers 25/2015*, S. 11.

<sup>17</sup> Brown, I. und Marsden C., *Regulating Code: Towards Prosumer Law?*, 25. Februar 2013, abrufbar unter <http://dx.doi.org/10.2139/ssrn.2224263> [abgerufen am 17. September 2016].

<sup>18</sup> „Im Jahr 1990 verzeichneten die drei Top-Automobilhersteller in Detroit zusammengenommen einen nominalen Umsatz von 250 Mrd. USD, bei einer Marktkapitalisierung von 36 Mrd. USD und 1,2 Millionen Beschäftigten. Im Jahr 2014 belief sich der Umsatz der drei Top-Unternehmen in Silicon Valley auf 247 Mrd. USD, bei einer Marktkapitalisierung von mehr als 1 Billion USD, aber nur 137 000 Beschäftigten“: „The Rise of the Superstars“, in *The Economist*, 17. September 2016.

<sup>19</sup> „Competition and privacy in markets of data“, Rede von Joaquín Almunia, Brüssel, November 2012; darin heißt es, dass „sich die GD Wettbewerb nun mit einem Fall befassen muss, in dem personenbezogene Daten verwendet

---

wurden, um gegen das EU-Wettbewerbsrecht zu verstoßen“; [http://europa.eu/rapid/press-release\\_SPEECH-12-860\\_en.htm](http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm) [abgerufen am 17. September 2016].

<sup>20</sup> In mehreren Studien wurde vorgebracht, dass verhaltensgesteuerte Märkte anfällig für Fehlentwicklungen sind, die sich nachteilig auf die gesellschaftliche Wohlfahrt auswirken, und dass ein Marktversagen bezüglich der Privatsphäre im Internet vorliegt, wenn ein auf verhaltensgesteuerter Werbung basierendes Geschäftsmodell „geradezu dafür geschaffen zu sein scheint, Vorteil aus der begrenzten Rationalität zu ziehen“. Siehe Borgesius, F. Z., „Behavioural Sciences and the Regulation of Privacy in the Internet“, in *Nudging and the Law – What can EU Law learn from Behavioural Sciences*; Acquisti, A., „The Economics of privacy and the economics of personal data“, *The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines*, 2010, <http://www.oecd.org/sti/ieconomy/46968784.pdf> [abgerufen am 17. September 2016].

<sup>21</sup> „Refining the EU merger control system“, Rede von Kommissarin Vestager, Studienvereinigung Kartellrecht, Brüssel, 10. März 2016.

<sup>22</sup> Zum europäischen menschenrechtsbezogenen Ansatz für den Schutz der Privatsphäre und personenbezogener Daten, der einen engen Bezug zu Menschenwürde und Selbstbestimmung aufweist, siehe beispielsweise *Consumer Privacy in Network Industries, A CERRE Policy Report*, 26. Januar 2016, S. 35 f.

<sup>23</sup> Urteil des EGMR vom 25. Februar 1997, Z/Finnland, Beschwerde Nr. 22009/93, Randnr. 95.

<sup>24</sup> Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Die Vorschrift, dass die Verarbeitung personenbezogener Daten nicht über den mit der Erhebung und/oder Weiterverarbeitung der Daten angestrebten Zweck hinausgehen darf, wurde bereits in der Richtlinie 95/46/EG in Erwägungsgrund 28 sowie in Artikel 6 Buchstabe b im Zusammenhang mit den Grundsätzen in Bezug auf die Qualität der Daten festgelegt.

<sup>25</sup> Artikel 5 Absatz 1 Buchstabe c sowie Artikel 14 und 15.

<sup>26</sup> Mit der Richtlinie 2011/83/EU über die Rechte der Verbraucher wurden die Richtlinie 97/7/EG über den Versandhandel und die Richtlinie 85/577/EWG über Haustürgeschäfte im Juni 2014 aufgehoben. Das EU-Verbraucherrecht wird derzeit im Rahmen des Programms REFIT einer umfassenden Überprüfung unterzogen. Die neue Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG wurde im Januar 2012 von der Kommission vorgeschlagen und schließlich am 4. Mai 2016 im Amtsblatt veröffentlicht.

<sup>27</sup> Urteil des Gerichtshofes vom 13. Mai 2014, Google Spain SL und Google Inc/Agencia Española de Protección de Datos (AEPD) und Mario Costeja Gonzalez, C-131/12, EU:C:2014:317. In dieser Rechtssache stellte der EuGH klar, dass ein Suchmaschinenbetreiber, dessen Tätigkeit auf die Einwohner eines EU-Mitgliedstaates ausgerichtet ist, den EU-Datenschutzvorschriften unterliegt.

<sup>28</sup> Bericht über den EDSB-Workshop „Privacy, Consumers, Competition and Big Data“, 2. Juni 2014; Workshop „Trading in Big Data: if data is the new oil, how should its extraction be regulated?“, Brunel University, London, 20. April bis 1. Mai 2015. In seinem im März 2016 erschienenen *Independent Review of UK Economic Statistics* schlägt Sir Charles Bean vor, den Konsum unentgeltlicher digitaler Produkte anhand des Wertes der im Internet verbrachten Zeit und der Zunahme des Internetverkehrs zu bemessen.

<sup>29</sup> „Müssten Amerikas Unternehmen die Preise senken, sodass ihre Profite auf das bislang übliche Niveau zurückgingen, könnten die von den Verbrauchern zu zahlenden Rechnungen um 2 % niedriger sein“: „The Problem with profits“, in *The Economist*, 26. März 2016.

<sup>30</sup> Siehe Stucke, M. E. und Grunes, A. P., „Big Data and Competition Policy“, in *OUP 2016*, S. 223 f.; „Too much of a good thing“, in *The Economist*, 26. März 2016.

<sup>31</sup> „... einige wenige Gatekeeper sind in der Lage, das Tracking und die Verknüpfung von ... Verhaltensdaten von Milliarden von Nutzern über Plattformen, Online-Dienste und Websites hinweg zu kontrollieren“: Acquisti, A., Taylor, C. und Wagman, L., *The Economics of Privacy*, in *Sloan Foundation Economics Research Paper*, Nr. 2580411, 8. März 2016, S. 3.

<sup>32</sup> Pew Resarch Centre, *News Use Across Social Media Platforms 2016*; siehe beispielsweise auch Pariser, E., *The Filter Bubble: What the Internet is Hiding from You*, 2011.

<sup>33</sup> „Facebook: Political bias claim ‚untrue‘“, in *BBC*, 10. Mai 2016; „Google bans payday lender advertising“, in *Financial Times*, 11. Mai 2016.

<sup>34</sup> Sind Eingriffe in die Vertraulichkeit der Kommunikation für die Erbringung einer Dienstleistung technisch erforderlich, sind grundsätzlich die Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation anwendbar (beispielsweise Artikel 2 Buchstabe g, Artikel 5 Absatz 1, Artikel 6 Absatz 5 sowie Artikel 9 Absätze 1 und 3). Zum Nutzen der in der Datenschutz-Grundverordnung vorgeschriebenen Einwilligung siehe Endnote 27 der vorläufigen Stellungnahme 5/2016 des EDSB zur Überprüfung der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG).

<sup>35</sup> Im Protokoll Nr. 27 zum Vertrag über die Europäische Union ist festgelegt, „dass der Binnenmarkt, wie er in Artikel 3 des Vertrags über die Europäische Union beschrieben wird, ein System umfasst, das den Wettbewerb vor Verfälschungen schützt“ und „für diese Zwecke die Union erforderlichenfalls nach den Bestimmungen der Verträge, einschließlich des Artikels 352 des Vertrags über die Arbeitsweise der Europäischen Union, tätig wird“.

---

Urteil des Gerichtshofes vom 6. Oktober 2009, GlaxoSmithKline Services u. a./Kommission u. a., C-501/06 P, C-513/06 P, C-515/06 P und C-519/06 P, EU:C:2009:610, Randnr. 61.

<sup>36</sup> In der Rechtsprechung des EuGH wird Fairness im Verbraucherrecht anhand des „Durchschnittsverbrauchers“ bewertet (Urteil des Gerichtshofes vom 16. Juli 1998, Gut Springenheide und Tusky/Oberkreisdirektor des Kreises Steinfurt, C-210/96, EU:C:1998:369, Randnr. 31); der Grundsatz der Verarbeitung personenbezogener Daten nach Treu und Glauben ist in Artikel 8 Absatz 2 der EU-Charta verankert; Artikel 101 und 102 AEUV über wettbewerbswidriges Verhalten und die missbräuchliche Ausnutzung einer beherrschenden Stellung nehmen ebenfalls auf das Gebot der Fairness Bezug.

<sup>37</sup> „Im Hinblick auf die Frage, inwieweit das Wettbewerbsrecht Märkte berücksichtigen muss, auf denen personenbezogene Daten eine Rolle spielen, argumentieren Wettbewerbswissenschaftler, dass personenbezogene Daten ebenso wie jede andere Ware oder Dienstleistung anhand ihrer wirtschaftlichen Merkmale analysiert werden sollten. Insofern könnten Datenschutzvorschriften lediglich den ‚rechtlichen Kontext‘ festlegen, in dem sich Wettbewerbsbeziehungen entfalten, und würden sich nicht von anderen Marktvorschriften unterscheiden. Die Datenschutzbehörden ihrerseits haben sich auf die Entwicklung der Leitprinzipien für ihren im Entstehen begriffenen Rechtsbereich konzentriert und sich kaum mit dessen Interaktion mit den älteren Bereichen des EU-Rechts befasst.“ Costa-Cabral und Lynskey, *The Internal and External Constraints of Data Protection on Competition Law in the EU*, S. 3. Zu den Schwierigkeiten natürlicher Personen, bei Verletzungen der Datenschutzvorschriften Schadenersatz zu erhalten, siehe Agentur für Grundrechte, *Access to data protection remedies in EU Member States*, Januar 2014.

<sup>38</sup> Die zentralen Ziele des Wettbewerbsrechts werden gegenwärtig diskutiert. Zur Verbraucherwohlfahrt als zentrales Ziel siehe die Urteile des Gerichtshofes in den Rechtssachen C-209/10, *Post Danmark*, und C-67/13, *Cartes Bancaires*; zu den Begriffen Wettbewerbsprozess und Wettbewerbsstruktur (soweit diese als Indikator für die Auswirkungen auf die Verbraucherwohlfahrt hinreichend geeignet sind) siehe die Urteile des Gerichtshofes in den Rechtssachen C-501/07 P, *Glaxo*, C-95/04, *British Airways*, und C/72.

<sup>39</sup> So gab beispielsweise die belgische Datenschutzkommission bei ICRI einen Bericht über die Geschäftsbedingungen von Facebook in Auftrag. Darin wurde festgestellt, dass die „Erklärung der Rechte und Pflichten“ des sozialen Netzwerks mutmaßlich gegen das europäische Verbraucherschutzrecht verstößt; <http://www.law.kuleuven.be/citip/en/news/item/facebook-revised-policies-and-terms-v1-3.pdf> [abgerufen am 17. September 2016].

<sup>40</sup> 14-MC-02 *Mesure conservatoire du 9 septembre 2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité*; *The Information Commissioner's response to the Competition and Market Authority's "Energy market investigation: notice of possible remedies" paper*, August 2015; Auditoraat Beslissing n° BMA-2015-P/K-28-AUD van 22 september 2015 Zaken MEDE-P/K-13/0012 en CONC-P/K-13/0013 *Stanleybet Belgium NV/Stanley International Betting Ltd en Sagevas S.A./World Football Association S.P.R.L./Samenwerkende Nevenmaatschappij Belgische PMU S.C.R.L. t. Nationale Loterij NV*; die Pressemitteilung zu der in Deutschland durchgeführten Untersuchung zu Facebook ist verfügbar unter [http://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2016/02\\_03\\_2016\\_Facebook.html](http://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2016/02_03_2016_Facebook.html) [abgerufen am 17. September 2016].

<sup>41</sup> Urteil des Gerichtshofes vom 23. November 2006, *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL/Asociación de Usuarios de Servicios Bancarios (Ausbanc)*, C-238/05, EU:C:2006:734.

<sup>42</sup> In den USA richtete die FTC ein Schreiben an die beiden fusionierenden Unternehmen, in dem diese nachdrücklich aufgefordert wurden, die Zusagen, die WhatsApp gegenüber seinen Kunden bezüglich seiner Datenschutzregelung gemacht hatte, auch weiterhin einzuhalten, auch wenn diese weiter gingen als jene, die bis dahin für Facebook-Nutzer galten. In diesem Schreiben wurde darauf hingewiesen, dass eine Verletzung dieser Zusagen einen Verstoß gegen Abschnitt 5 des FTC Act darstellen würde, der unlautere oder irreführende Geschäftspraktiken verbietet. In ihrer Entscheidung über die geplante Fusion erklärte die Kommission: „Datenschutzspezifische Bedenken, die sich aus dem Umstand ergeben, dass nach dem geplanten Zusammenschluss größere Datenmengen unter der Kontrolle von Facebook stehen werden, fallen nicht in den Anwendungsbereich des EU-Wettbewerbsrechts, sondern in den Anwendungsbereich des EU-Datenschutzrechts“; Entscheidung der Kommission vom 3. Oktober 2014 zur Erklärung der Vereinbarkeit eines Zusammenschlusses mit dem Gemeinsamen Markt (COMP/M.7217 – FACEBOOK/WHATSAPP) gemäß der Verordnung (EG) Nr. 139/2004 des Rates. Siehe „What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU merger case“, in Europäische Kommission, *Competition merger brief*, Ausgabe 1/2015, S. 7.

<sup>43</sup> „Facebook Grilled by EU's Vestager Over WhatsApp Merger U-Turn“, 9. September 2016, <http://www.bloomberg.com/news/articles/2016-09-09/facebook-grilled-by-eu-s-vestager-over-whatsapp-merger-u-turn> [abgerufen am 17. September 2016].

<sup>44</sup> Urteil des Gerichtshofes vom 15. Februar 2005, *Kommission/Tetra Laval*, C-12/03 P, EU:C:2005:87.

<sup>45</sup> Erläuterungen zur Rechtsprechung des EuGH, in der die öffentliche Ordnung als mögliche Begründung für die Feststellung von Verstößen gegen das Wettbewerbsrecht und der Schutz der Grundrechte im Rahmen der

---

Rechtsprechung zum Binnenmarkt herangezogen wurde, sind beispielsweise Costa-Cabral und Lynskey, S. 29 ff., zu entnehmen.

<sup>46</sup> „Unbeschadet der Absätze 1 und 2 können die Mitgliedstaaten geeignete Maßnahmen zum Schutz anderer berechtigter Interessen als derjenigen treffen, welche in dieser Verordnung berücksichtigt werden, sofern diese Interessen mit den allgemeinen Grundsätzen und den übrigen Bestimmungen des Gemeinschaftsrechts vereinbar sind.“ Als berechnete Interessen werden dabei ausdrücklich die „öffentliche Sicherheit“ (1), die „Medienvielfalt“ (2) und die „Aufsichtsregeln“ (4) genannt (Artikel 21 Absatz 4 der Verordnung 139/2004). [http://ec.europa.eu/competition/publications/cpn/2005\\_1\\_19.pdf](http://ec.europa.eu/competition/publications/cpn/2005_1_19.pdf);

[http://ec.europa.eu/information\\_society/media\\_taskforce/doc/pluralism/media\\_pluralism\\_swp\\_en.pdf](http://ec.europa.eu/information_society/media_taskforce/doc/pluralism/media_pluralism_swp_en.pdf) [abgerufen am 17. September 2016].

<sup>47</sup> „Antitrust, Privacy and Big Data“, *Concurrences*, 3. Februar 2015; Gemeinsamer Workshop des EDSB und der ERA, „Competition Rebooted: enforcement and personal data in Digital Markets“, 24. September 2015, Brüssel; Rundtischgespräch bei der *Autorité de la Concurrence*, 8. März 2016, Paris.

<sup>48</sup> Siehe *BEUC Strategy, A Consumer-Driven Digital Single Market*, September 2015: „Für Verbraucher ist es [in Online-Umgebungen] häufig schwierig, sich zurechtzufinden, ihre Optionen und Rechte zu verstehen und Lösungen zu finden, wenn etwas falsch läuft.“

<sup>49</sup> COM (2016)288, Mitteilung der Kommission, „Online-Plattformen im digitalen Binnenmarkt, Chancen und Herausforderungen für Europa“.

<sup>50</sup> Entschließung der Frühjahrskonferenz der Datenschutzbehörden, Mai 2016, verfügbar unter <http://www.naih.hu/budapest-springconf/files/Resolution---new-frameworks.pdf> [abgerufen am 17. September 2016]. Siehe auch die Antwort des EDSB auf die öffentliche Konsultation der Kommission zum Regelungsumfeld für Plattformen, Online-Vermittler, Daten, Cloud-Computing und die partizipative Wirtschaft, 15. Dezember 2015; House of Lords, Select Committee of the European Union, *10th Report of Session 2015-16, Online Platforms and the Digital Single Market*, 20. April 2016.

<sup>51</sup> Hijmans, H., *The European Union as a constitutional guardian of Internet privacy and data protection*, S. 63 ff., <http://hdl.handle.net/11245/1.511969> [abgerufen am 17. September 2016]. (Eine geänderte Fassung dieser Dissertation sollte im Sommer 2016 bei Springer International Publishing unter dem Titel *The European Union as Guardian of Internet Privacy* erscheinen).

<sup>52</sup> JRC Technical Reports, Institute For Prospective Technological Studies Digital Economy Working Paper 2016/05, *An Economic Policy Perspective On Online Platform*, S. 42 f.; <https://ec.europa.eu/jrc/sites/jrcsh/files/JRC101501.pdf> [abgerufen am 17. September 2016].

<sup>53</sup> EU-Kartellbeschwerde von Disconnect gegen Google, Juni 2015; der vollständige Wortlaut der Beschwerde ist verfügbar unter <https://www.documentcloud.org/documents/2109044-disconnect-google-antitrust-complaints.html> [abgerufen am 17. September 2016].

<sup>54</sup> Consumer Justice Enforcement Forum (CoJEF), *Enforcement of Consumer rights: strategies and recommendations*, Mai 2016.

<sup>55</sup> Der vollständige Bericht über die Studie ist verfügbar unter [http://fbrno.climg.no/wp-content/uploads/2014/02/2014-05-14-Unfair-cloud-storage-terms\\_report.pdf](http://fbrno.climg.no/wp-content/uploads/2014/02/2014-05-14-Unfair-cloud-storage-terms_report.pdf) [abgerufen am 17. September 2016].

<sup>56</sup> Urteil des Gerichtshofes vom 28. Juli 2016, Verein für Konsumenteninformation/Amazon EU Sàrl, C-191/15, EU:C:2016:612.

<sup>57</sup> Präsident Junckers politische Leitlinien, 15. Juli 2014, [https://ec.europa.eu/priorities/publications/president-junckers-political-guidelines\\_de](https://ec.europa.eu/priorities/publications/president-junckers-political-guidelines_de) [abgerufen am 16. September 2016]; Antwort des BEUC auf die Konsultation zur „Stärkung der nationalen Wettbewerbsbehörden zur wirksameren Durchsetzung des EU-Wettbewerbsrechts“, 2016.

<sup>58</sup> Eurobarometer Spezial 431, Datenschutz, Juni 2015. Siehe auch die in jüngerer Zeit von Opinium Research durchgeführte Erhebung unter 7000 Befragten in Europa sowie im Nahen und Mittleren Osten, die ergab, dass 75 % der Verbraucher kein Vertrauen in den Datenschutz bei Social-Media-Marken und Marketing-Unternehmen haben; <https://f5.com/about-us/news/press-releases/european-and-middle-eastern-consumers-deeply-conflicted-over-privacy-and-security-priorities-19968> [abgerufen am 17. September 2016]; die Europäische Kommission stellte fest, dass „das Internet künftig nur erfolgreich sein kann, wenn die Verbraucher Vertrauen in die Online-Plattformen haben und diese alle geltenden Rechtsvorschriften sowie die berechtigten Interessen der Verbraucher und anderen Nutzer respektieren“: Arbeitsdokument der Kommissionsdienststellen, *Online Platforms Accompanying the document Communication on Online Platforms and the Digital Single Market*, S. 44. Siehe auch die Rede von Kommissarin Vestager mit dem Titel „Making data work for us“, Data Ethics event on Data as Power, Kopenhagen, 9. September 2016: „Verbraucher nutzen Suchmaschinen ... [und] ... soziale Netzwerke... Und sie bezahlen keinen Cent für diese Dienstleistungen. Stattdessen bezahlen sie mit ihren Daten. Das kann unproblematisch sein, solange die Menschen damit zufrieden sind, dass die Daten, die sie offenlegen, einen fairen Preis für die Dienstleistungen darstellen, die sie dafür erhalten. Personenbezogene Daten sind mittlerweile ein wertvolles Gut. Dies kann aber langfristig nur so bleiben, wenn die Menschen den Unternehmen, die ihre Daten erheben, im Hinblick auf die Art der Nutzung dieser Daten vertrauen. Und dieses Vertrauen besteht noch nicht.“

<sup>59</sup> „Keines der im Index vertretenden Unternehmen bietet seinen Nutzern hinreichend klare, umfassende und zugängliche Informationen über seine die Meinungsfreiheit und Privatsphäre berührenden Praktiken. Dies betrifft unter anderem Informationen über den Umgang mit Nutzerdaten, die Durchsetzung der Nutzungsbedingungen sowie behördliche und private Anfragen“; <https://rankingdigitalrights.org/index2015/findings/> [abgerufen am 17. September 2016].

<sup>60</sup> Vorläufige Stellungnahme des EDSB zur Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG), 22. Juli 2016, S. 14 ff.

<sup>61</sup> Urteil des Gerichtshofes vom 9. November 1983, Michelin/Kommission, C-322/81, EU:C:1983:313, Randnr. 70; siehe auch S. 20 der vorläufigen Stellungnahme des EDSB.

<sup>62</sup> Ein Großteil der Debatte über Technologien zur Erkennung von Werbeblockern drehte sich auch um die Frage, ob im Rahmen der Prüfung, ob Werbung angezeigt werden kann, eine Speicherung personenbezogener Daten gemäß Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation erfolgt und infolgedessen für den Einsatz von Werbeblockern die Zustimmung des Nutzers eingeholt werden muss.

<sup>63</sup> Das Projekt mit dem Titel „Solid“ (abgeleitet von „social linked data“ [sozial vernetzte Daten]) wird beschrieben als eine „Reihe vorgeschlagener Konventionen und Instrumente für den Aufbau dezentraler Web-Anwendungen auf der Grundlage der Linked-Data-Prinzipien. Solid ist modular aufgebaut und erweiterbar. Es basiert weitestmöglich auf den vorhandenen W3C-Standards und -Protokollen“; <https://github.com/solid/solid> [abgerufen am 17. September 2016].

<sup>64</sup> OECD, *The Role and Measurement of Quality in Competition Analysis*, 2013.

<sup>65</sup> House of Lords Report, S. 102. Siehe Ezrachi, A. und Stucke, M. E., „The Curious Case of Competition and Quality“, in *Journal of Antitrust Enforcement*, 2015, 1.

<sup>66</sup> Consumer Justice Enforcement Forum (CoJEF), *Enforcement of Consumer rights: strategies and recommendations*, Mai 2016.

<sup>67</sup> Siehe beispielsweise Evans, D. S., „Antitrust Economics of Free“, in *Competition Policy International, Spring 2011*, 17. April 2011; Newman, J. M., „Antitrust in Zero-Price Markets: Foundations“, in *University of Pennsylvania Law Review*, Bd. 164, 31. Juli 2014; University of Memphis, *Legal Studies Research Paper*, Nr. 151: „Werden keine Marktanalysen durchgeführt, besteht die Möglichkeit, dass aufgrund einer systematisch unzureichenden Durchsetzung der Kartellgesetzgebung ein massiver Schaden für die Verbraucherwohlfahrt entsteht.“

<sup>68</sup> Im Zuge dieser Ermittlung prüften 25 Behörden 330 Websites, über die digitale Inhalte verkauft werden, und stellten fest, dass die Hälfte von ihnen unlautere Vertragsbedingungen oder unklare Informationen über das Rücktrittsrecht der Nutzer sowie unvollständige Angaben über die Identität der Händler und die Kontaktmöglichkeiten enthielten: *SWEEP on Digital Content* [Sweep zu digitalen Inhalten] des Netzwerks für die Zusammenarbeit im Verbraucherschutz; [www.ec.europa.eu/consumers/strategy.../policy.../consumer\\_policy\\_report\\_2014\\_en.pdf](http://www.ec.europa.eu/consumers/strategy.../policy.../consumer_policy_report_2014_en.pdf) [abgerufen am 17. September 2016].

<sup>69</sup> Mitteilung der Kommission – Erläuterungen zu den Prioritäten der Kommission bei der Anwendung von Artikel 82 des EG-Vertrags auf Fälle von Behinderungsmissbrauch durch marktbeherrschende Unternehmen, ABl. C 45 vom 24.2.2009, S. 7.

<sup>70</sup> Entscheidung in der Sache Google/DoubleClick, Randnr. 39. Vertikale Integration und Konzentration werden im gemeinsamen Bericht der französischen und der deutschen Wettbewerbsbehörde *Competition Law and Data*, 10. Mai 2016, S. 16 ff., erläutert. Edelman, B. G., „Does Google Leverage Market Power through Tying and Bundling?“, in *Journal of Competition Law and Economics*, Bd. 11, Ausgabe 2, Juni 2015. Zur Marktmachtübertragung siehe Competition and Markets Authority, *The commercial use of consumer data: Report on the CMA's call for information*, Mai 2015, Randnrn. 3.60 und 3.61.

<sup>71</sup> Siehe Anmerkung 40 oben.

<sup>72</sup> Siehe Cohen, J. E., *Irrational Privacy?*, 2012; Akerlof, G., „The Market for Lemons, Qualitative Uncertainty and the Market Mechanism“, in *Quarterly Journal of Economics*, 84 (3), 1970, S. 488 ff.; Ryan Calo, R., „Privacy and Markets: A Love Story“, in University of Washington School of Law, *Legal Studies Research Paper*, Nr. 2015-26, S. 27. David A. Friedman zufolge findet eine „irreführende Umrahmung“ unentgeltlicher Produkte statt, die den Verbraucher in seiner Entscheidungsfindung täuscht; *Free Offers: A New Look*, New Mexico Law Review, Bd. 38, 2008, S. 49 ff., S. 68 f.

<sup>73</sup> Mitteilung der Kommission über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre (KOM(2007) 228 endgültig); zum Markt für Technologien zum Schutz der Privatsphäre siehe beispielsweise „Hiding from big data“, in *The Economist*, 7. Juni 2014.

<sup>74</sup> CMA, *The commercial use of consumer data*, Randnr. 3.21; Executive Office of the President, President's Council of Advisors on Science and Technology, *Report to the President, Big data and Privacy: a technological perspective*, Mai 2014.

<sup>75</sup> Vorläufige Stellungnahme des EDSB zur Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation.

---

<sup>76</sup> Siehe die Stellungnahmen des EDSB zum Weg zu einem neuen digitalen Ethos und Big Data. Siehe ferner den CERRE-Bericht *Consumer Privacy in Network Industries, Improving Network industries regulation*, Januar 2016; Costa-Cabral und Lynskey, S. 15: „unter bestimmten Umständen kann der Datenschutz eine wichtige normative Benchmark für das Wettbewerbsrecht bieten“; Fairfield, J. A. T. und Engel, C., „Privacy as a Public Good“, in *Duke Law Journal*, Bd. 65, Dezember 2015, Nr. 3.

<sup>77</sup> Urteil des Gerichtshofes vom 15. Januar 2014, Association de médiation sociale/Union locale des syndicats CGT u. a., C-176/12, EU:C:2014:2, Randnr. 42. Des Weiteren wurde vorgebracht, dass die in der Charta festgelegten Verpflichtungen nicht nur auf den öffentlichen Sektor anwendbar sind, sondern auch auf „horizontale“ Beziehungen zwischen natürlichen und juristischen Personen: „Ein Grundrecht wäre unwirksam, wenn es ausschließlich vor Behörden schützen würde“, Hijmans, S. 43 ff.

<sup>78</sup> AEUV, Artikel 7. In seinem Urteil vom 19. Februar 2002 in der Rechtssache C-309/99, J. C. J. Wouters/Algemene Raad, verfolgte der Gerichtshof einen Ansatz, der ein Gleichgewicht zwischen dem Schutz der Struktur des Marktes und den die öffentliche Ordnung betreffenden Zielen der Rechtspflege wahren soll.

<sup>79</sup> Entschließung des Europäischen Parlaments vom 19. Januar 2016, *Auf dem Weg zu einer Akte zum digitalen Binnenmarkt*, Randnr. 12.

<sup>80</sup> Vorläufige Stellungnahme des EDSB, 2014, S. 34; House of Lords Digital, S. 47; Monopolkommission, Sondergutachten 68, *Wettbewerbspolitik: Herausforderung digitale Märkte*, S. 160 f.

<sup>81</sup> Verordnung (EG) Nr. 139/2004 des Rates vom 20. Januar 2004 über die Kontrolle von Unternehmenszusammenschlüssen, Artikel 21 Absatz 4.

<sup>82</sup> Der Begriff „Clearinghaus“ bezeichnet eine zentrale Agentur oder informelle Vermittlungsstelle, über die Abrechnungen abgewickelt, Informationen verbreitet oder Unterstützungsleistungen koordiniert werden, um für eine erhöhte Wirksamkeit und Stabilität zu sorgen. Gemeinhin wird er mit dem Kauf und Verkauf von Finanzinstrumenten in Verbindung gebracht, es gibt jedoch auch zahlreiche Beispiele für Clearinghäuser in den unterschiedlichsten Sektoren, wie beispielsweise in den Bereichen Eisenbahn und Bildung, aber auch im Datenschutz und beim Zugang zu Informationen.

<sup>83</sup> Costa-Cabral und Lynskey weisen darauf hin, dass es mit dem Urteil des Gerichtshofes vom 14. März 2013, Allianz Hungária Biztosító u.a., C-32/11, EU:C:2013:160, möglicherweise bereits einen Präzedenzfall gibt, in dem ein anderer Rechtsbereich herangezogen wurde, um eine bezweckte Beschränkung festzustellen.

<sup>84</sup> Urteil des EGMR vom 24. Juni 2004, von Hannover/Deutschland, Beschwerde Nr. 59320/00; Urteil des EGMR vom 2. Dezember 2008, K.U./Finnland, Beschwerde Nr. 2872/02, Randnrn. 43 und 48.

<sup>85</sup> „Ein engerer Dialog zwischen Behörden aus unterschiedlichen Sektoren könnte zu der Bildung von globalen Partnerschaften führen, deren Notwendigkeit zunehmend erkannt wird und die eine Art von Gemeinschaftsbereich offener Daten schaffen können, in dem Daten und Ideen wie beispielsweise Statistiken und Landkarten mit geringerem Überwachungsrisiko frei fließen können, zur Verfügung stehen und im öffentlichen Interesse ausgetauscht werden können, so dass der Einzelne mehr Einfluss über Entscheidungen hat, die ihn betreffen“: Stellungnahme des EDSB, *Der Weg zu einem neuen digitalen Ethos*, S. 12 und Fußnote 36, in der mehrere Quellen aufgeführt sind, in denen diesbezüglich ähnliche Vorstellungen vertreten werden; Schneier, B., *Data and Goliath, the hidden battles to collect your data and to control your world*, 2015.

<sup>86</sup> Siehe beispielsweise, Andrejevic, M., „Surveillance in the digital enclosure“, in *The Communication Review*, Bd. 10, S. 295 ff.; Zittrain, J., *The future of the Internet and how to stop it*, 2008.

<sup>87</sup> So wurde beispielsweise im Laufe eines im Jahr 2015 von der norwegischen Datenschutzbehörde und einem Mitglied des norwegischen Technologierates organisierten Seminars zum Thema Privatsphäre der Gedanke thematisiert, die Vergabe von Domainnamen an die rechtlich verbindliche Verpflichtung zu koppeln, die mit ihrer Nutzung verbundenen strengen Vorschriften im Hinblick auf Privatsphäre und Sicherheit einzuhalten <http://www.zdnet.com/article/how-two-remote-arctic-territories-became-the-front-line-in-the-battle-for-Internet-privacy/> [abgerufen am 17. September 2016].